OFFICE OF DATA DISCOVERY FORENSIC ANALYSIS

DIGITAL +1

Issue 1 - Aug 2021

BAD APPLE, INC.

Apple to Systematically Scan, NeuralHash, Flag, Human Review, and Report Your Photos to the FBI

Publisher

Retired FBI special agent Jane Mason is the CEO of the successful private investigation firm Secure Investigation® d/b/a Office of Data Discovery Forensic Analysis, LLC. Co-founded in 2014 with a fellow retired FBI special agent, Secure Investigations® focuses on advancing the professional teamwork, networking, and camaraderie of former FBI special agents.

An expert in white-collar crime investigation, Ms. Mason has extensive experience in the investigation, collection, and management of forensic evidence, including hundreds of cases involving mortgage fraud, environmental crimes, financial institution fraud, public corruption, money laundering, structuring, Ponzi schemes, fraud against the government, and civil rights violations. She is the recipient of numerous awards and commendations, including an award from the United States attorney general in recognition of her outstanding investigative skills, leadership, teamwork, and successful liaisons.

Publisher

David is President of Secure Investigation® d/b/a Office of Data Discovery Forensic Analysis, LLC. He is also the founder and president of Mon Ethos Pro Consulting and USVI News, and has been CTO to a number of digital development and technology firms.

In cooperation with the US Attorney's Office, David's experience and technical know-how resulted in a half-billion-dollar forfeiture, one of the largest in our nation's history.

He has lectured on cybersecurity, AI, virtual reality, mobile app development, and e-discovery.

David has an uncanny ability to recognize and capture the mechanics of how our real lives are changing, improving, and growing through our use of and experience with the online digital universe.

Contributors

Charlene Collazo Goldfield, Esq.

A graduate of American University Washington College of Law, Attorney Goldfield recently earned her LLM in national security and cybersecurity law from George Washington University Law School. While in her LLM program, she published a paper titled "The Right to be Forgotten and its Unintended Consequences to Intelligence Gathering." She also holds dual degrees in print journalism and political science from Florida International University.

Attorney Goldfield is currently an Attorney Advisor with the Public Safety and Homeland Security Bureau at the Federal Communications Commission and also teaches graduate courses for the Department of Public Policy and Administration at Florida International University, including one on administrative law, policy, and emerging technologies. She serves as the Young Lawyer's Division Liaison for the Cybersecurity Legal Task Force and the Co-Chair of the Section of Science and Technology at the American Bar Association. Charlene was a law clerk with the district court of Maryland for Montgomery County and the Superior Court for the District of Columbia.

Disclaimer: The views expressed in this article do not necessarily represent the views of the Public Safety & Homeland Security Bureau of the Federal Communications Commission or the United States.

Muhammad A. Rushdi, PhD

Muhammad A. Rushdi received BSc and MSc degrees in biomedical engineering and systems and a BSc degree in mathematics from Cairo University, Giza, Egypt. He received his MSc and PhD degrees in computer and information science and engineering from the University of Florida at Gainesville.

He is currently an associate professor at the Department of Biomedical Engineering and Systems at Cairo University, Giza, Egypt. Muhammad's research interests include biomedical signal processing, information security and forensics, machine learning, image processing, computer vision, and applied mathematics. He is also a freelance technical writer and editor with over forty peer-reviewed publications.

He has been co-advisor to more than twenty MSc and PhD students and has received research and development support from EACEA, ITIDA, Flat6Labs, and French Tech Ticket.

Jamilia Grier, Esq.

Attorney Grier is a privacy and regulatory attorney with over fifteen years of experience; she is licensed in New York and Connecticut. She has worked in a wide range of industries including financial services, technology, hospitality, and manufacturing. She is also experienced in working with different countries and cultures and has significant expertise in cross-border transactions. She handles matters concerning corporate law and contracts and is well-versed in data privacy and protection.

She currently serves as CEO and managing partner of ByteBao. Her experience includes leading Data & Privacy Operations at Standard Chartered Bank and the Legal Compliance team for Marriott International based out of China and Singapore.

Joseph Balliro Jr., Esq.

Joseph J. Balliro, Jr. has been a practicing trial attorney in the Commonwealth of Massachusetts and nationwide for over three decades. He has a wide range of experience in federal and state courts.

Attorney Balliro has handled complex electronic discovery disclosures and has successfully defended clients using the sophisticated services offered by Office of Data Discovery. He is well versed in ISO compliance and internal security for high-risk assets.

Greg Tanaka, PhD

In the fields of electrical engineering and computer science, Greg is an alumnus of both Caltech and the University of California, Berkeley; he also participated in SITN at Stanford University.

He is the founder and CEO of Percolata, a machine-learning-based forecasting service that gives time series forecasts with error rates one-third to one-fourth the rates of traditional time series forecasting methods. Greg leads all business and technical activities at Percolata and helped raise ten million dollars from top-tier venture investors including Google Venture, Andreesen Horowitz, and Menlo Ventures. He also started Pika Group, a subsidiary of Percolata that does algorithmic trading using machine learning models.

Greg also teaches a machine learning course on algorithmic trading and is one of the top machine learning consultants on Upwork. He ranked in the top five percent in a prestigious Kaggle time series forecasting competition.

John H. Halpern, M.D.

Dr. John Halpern, a practicing psychiatrist physician, has spent more than twenty years of his career at McLean Hospital and Harvard Medical School. He was director of the Laboratory for Integrative Psychiatry, Division of Alcohol and Drug Abuse, at McLean Hospital. Dr. Halpern was also an assistant professor of psychiatry at Harvard Medical School. During this academic period, he provided supervision and training on psychiatry and addiction psychiatry within various Harvard-Medical-School-affiliated training programs.

Dr. Halpern is a leading expert in the field of psychiatry and substance-dependence drug development and research review for the Gerson Lehrman Group.

Dr. Halpern is frequently sought as an invited lecturer and as a forensic expert, and his work has been featured in leading publications such as Newsweek, National Geographic, Discover Magazine, Wired, The New York Times, and numerous medical journals.

Contributors

Sajid Ahmed

Sajid Ahmed is currently a PhD software engineering student at Yangzhou University China. He is a lecturer in the computer science department at Shah Abdul Latif University, Khairpur, Sindh, Pakistan. His research interests are machine learning, software engineering, human factors in software engineering, Automatic Features Learning, and vulnerability detection. He has more than five years of experience in the software industry and university teaching and has published various research articles in the computer science and software engineering domains.

Joe Leonard

A graduate of the University of Virginia, Joe is a freelance writer living in Los Angeles, CA. He writes an online blog that has been active for over six years. He posts topical, emotionally powerful articles and essays, often with an emphasis on comedy. He has also written episodic television and several short films.

Different Kinds of Apples

Stroll through the produce section in your local grocery store and you'll most likely be faced with a choice between several different varieties of apples. While the visual differences between a Granny Smith and a Red Delicious apple may be few, there are plenty of subtle differences that cannot be picked up by the naked eye alone. Consider how distinct the tastes, textures, and consistencies of these two kinds of apples are.

Many people know the difference between various types of apples by their touch, taste, and smell. But how capable is an algorithm of categorizing and labeling images based on these subtle differences? Apple Inc. is attempting to use technology to do just that.

Apple Inc. has just announced that iOS 15 will include the capability to scan, detect, and flag iCloud images that potentially represent child sexual abuse materials (CSAM). This update is based on a "hashing" computer technique for comparing images on an iCloud user account against a child abuse material image database.

This image database receives its image data from child-safety organizations, primarily the National Center for Missing and Exploited Children (NCMEC), which acts as the comprehensive reporting center for child abuse material and works in collaboration with law enforcement agencies across the United States. In the event that child abuse material is detected, Apple will report these instances to NCMEC.

Historically, Apple's emphasis on privacy and its unwillingness to compromise the security of its devices has led customers to almost blindly trust the company. Now the question becomes: has that trust been well earned? Apple's massive collection and storage of customer images has allowed for the development of powerful machine learning algorithms that could potentially infringe upon customer privacy.

A Departure from Apple's Traditional Privacy Focus

To understand the significance of Apple's new child abuse material detection policy, we must look at how the company has previously dealt with photos and encryption on its devices. While almost everything on an iPhone is encrypted, from your photos and calendar to your notes and reminders, there are a few notable exceptions.

Apple encrypts your mail as you send it; but at rest on a mail server, mail is not encrypted. The company requires you to manually select a setting to encrypt mail stored on IMAP mail servers. Other exceptions to Apple's encryption standards are text messages and, to some extent, iMessages.

When a text message is sent using an Apple device, the text message is not encrypted. An iMessage, on the other hand, is encrypted. There is a glaring hole in the encryption of iMessages, however, which is that the encryption key for iMessages is included on the cloud when you use the "Messages in iCloud" option. This means that Apple has access to your encrypted messages and the key with which to decrypt them; this could lead to your iMessages being decrypted anyway. In order to fully encrypt your iMessages and keep them from being decrypted, you are required to turn off this option. This will then lead to a new encryption key that Apple doesn't have.

Apple would argue that the collection of data about user images is meant to provide a better user experience. For example, Apple needs to collect

information about user images to identify people in photos and enable users to sort their photos by location. While this feature is meant to improve user experience, unfortunately, it results in copious amounts of data being gathered from your photos.

Apple's new child abuse material detection plan builds upon this already shaky foundation of privacy violations and takes it to whole new extremes.

What Is the Technology Behind Apple's Child Abuse Material Detection Initiative?

"AI is revolutionary, but it also requires a level of human intervention. That is why there is still room for growth in understanding and learning about these types of algorithms because it can have some serious implications on an individual, including their privacy and civil liberties." —Charlene C. Goldfield, an attorney with the U.S. Federal Government

We've talked about how this is a huge departure from how Apple has historically handled customer privacy. Now, let's look at how the technology works. Professor Muhammad Rushdi, PhD, associate professor at the Department of Biomedical Engineering and Systems at Cairo University, breaks it down for us.

"The child abuse material detection technology essentially works as follows," says Rushdi. "First of all, for each of the child abuse material database images, a small fixed-size chunk of data, called an image hash, is generated through a hashing process which captures the key image features. This process ensures that images of different content have different hash values, while highly similar images have identical hash values irrespective of variations in scale, resolution, color, quality, or degree of blurring. The same hashing process is applied to the images available on an iCloud user account.

"Secondly, a comparison is carried out on the user device among the hash values associated with the child abuse material database images and the iCloud ones. A cryptography technique is employed to encrypt and conceal the matching result, the image hash, and other image information. Hence, a safety voucher is generated and uploaded along with each image to iCloud. Thirdly, a secret sharing scheme is employed to ensure that Apple can't reveal the contents of the uploaded safety vouchers as long as a specified child abuse material image count isn't reached. Once this count is exceeded, the 'shared secret' is revealed and Apple can then recover and manually review the child abuse material image data before reporting the case to NCMEC and law-enforcement authorities."

Let's illustrate the repercussions of Apple's new technology with the following example. Assume that the green-apple photo comes from the child abuse material database while the red-apple photo is on an iCloud user's account. The hashing process is carried out using Apple's NeuralHash technology, which is based on brain-like artificial neural networks that are taught, using possibly thousands of examples, to map an image to a small fixed-length hash value.

When it looks at the green-apple image, the NeuralHash technology will most likely identify the salient image objects, which would be the hand and the apple. It will ignore the unimportant black background. Next, the key geometrical features of the hand and the apple are captured and encoded as a hash value. For the red-apple photo, a similar process will be carried out. The differences between the two photos in terms of apple color and location are most likely going to be ignored. This means that the two photos are going to have identical (or almost identical) hash values, resulting in the red-apple photo being flagged as child abuse material.

This illuminates a key problem with the introduced technology. The matching process focuses only on the image content, completely disregarding color and location information. It also ignores the identity and profession of the user, which is extremely important when the user is a lawyer or a doctor with legitimate access to child abuse material images.

For example, a red-apple photo on a lawyer's account will have the same hash value as a green-apple photo on a sex offender's account, leading to both photos being flagged as potentially illegal child abuse material. Because of the fallibility of Apple's human review process, the subsequent manual review isn't guaranteed to resolve any confusion. This could put the reputation of the lawyer in jeopardy over Apple's mistake.

The potential for a false positive is likely greater than the one-in-a-trillion chance Apple theorizes. According to Greg Tanaka, PhD, CEO and Founder of Percolata, “An image might generate a vector for a ‘child’ if there is a child in the image and ‘naked’ if there is someone that is naked in the image. Depending on how this was done, these representations might be of a naked child or a child with another person that is naked. Just as the Google Translate process is reversible, so is the process of going from the mathematical representation to the image. However, child abuse material detection will drop a certain number of these mathematical representations.”

Apple’s report on its CSAM detection technology doesn’t specify what mathematical representations get dropped in child abuse material detection, which means that we can’t know the accuracy of the technology or the security of the encryption process. If Apple were to make its child abuse material detection tools open-source, then the public would be able to determine what an Apple employee could really see and how close it was to the original image. Until then, we’re left wondering what gets dropped during the child abuse material detection process and how often a false positive is actually likely to occur.

Apple's intention to prevent the abuse of children is no doubt a noble venture. However, the reality is that its new child abuse material policy raises several alarming legal and ethical concerns.

Not only could this policy compromise customer privacy and data security, but Apple's child abuse material detection process is murky at best. Apple risks trampling on the protections afforded to attorney-client and physician-patient relationships. Who is to blame if Apple's child abuse material detection technology results in compromised attorney-client privilege amidst a trial or a HIPAA violation due to leaked patient data? Apple's child abuse material detection technology will have far-reaching effects that have not yet been fully appreciated.

At the beginning of this article, we illustrated how an algorithm might not be able to tell the subtle difference between two kinds of apples based simply on appearance. Similarly, the algorithm in Apple's new child abuse material detection technology may not be able to tell the difference between two images on a user device. Nor will it be able to tell the difference between images on the device of a healthcare professional, who possesses them for legitimate medical purposes, and images on a device belonging to an actual sex offender.

Legal and Ethical Considerations

The legal concerns raised by Apple's new child abuse material policy are numerous. For one, Apple does not own the rights to the photos it is scanning. Apple's use of this technology to access images, process them in a way that has little to do with the service being provided, and share those images with a third party (and potentially a law enforcement agency) raises copyright, fair use, and intellectual property concerns.

There are also numerous data privacy and data ethics concerns. As data privacy laws in the United States are evolving, and there is no overarching federal data privacy regulation, people have either limited or no protection against potential invasions of privacy under Apple's new policy.

Apple's new child abuse material detection technology is testing the limits and sufficiency of state and Constitutional protections. In essence, while Apple is not an arm of the U.S. government, the company may be compromising Fourth Amendment protections by searching and seizing private property and passing it on to law enforcement.

According to Jamilia Grier, CEO and Founder of ByteBao, a data privacy and protection consultancy based in Singapore, "Apple is overstepping its

bounds by blurring the lines between product/service provider and law enforcement. Of course, Apple has a corporate social responsibility to minimize the child abuse material supply on its cloud, but they have now taken on an additional role of proactively coordinating with law enforcement."

"We note that this is a major deviation from Apple's past relationship with law enforcement, most notably with their refusal to assist the FBI with extracting information from a phone belonging to the terrorists responsible for the 2015 San Bernardino attack. Now, however, it seems that Apple has reversed course and is beginning to act as an agent of the government in monitoring and reporting child abuse material," says retired FBI Special Agent Jane Mason, owner and CEO of Secure Investigation.

Mason continued, "As a retired FBI Special Agent, I am 100% behind legal and ethical initiatives to bring pedophiles to justice.

Historically, probable cause has been required before our private information, including the photos on our phones, could be reviewed by law enforcement.

What if the Algorithm Makes a Mistake?

According to Greg Tanaka, "Roughly 1.4 trillion photos are taken a year and increasing, so there is a chance that some low number of innocent person(s) each year will unfortunately get mistakenly ensnared as a child pornographer even for images with no naked children." In other words, due to the sheer volume of images that will be impacted by Apple's CSAM policy, there are bound to be errors.

There is also an ethical concern with the arbitrary nature of Apple's child abuse material threshold. Under Apple's new policy, an account will only be flagged if a threshold number of images match the child abuse material image database. This means that Apple determines how many matches are required before an account is flagged and they notify NCMEC. If that threshold is not met, then the matches are not reported.

It is unclear what this threshold is and how Apple calculated this number. It is also unclear what responsibility Apple holds for matches found in numbers below the threshold that would trigger the flagging of an account.

In Apple's defense, their threshold is in place in order to reduce the probability of a given account being incorrectly flagged (Apple states the likelihood of this occurring to be one in a trillion). But this threshold raises a whole host of further questions. How many child abuse material matches need to occur before an account is flagged for review? And, if the threshold is too high and Apple misses an account that should have been flagged, could this be deemed as negligence on their part?

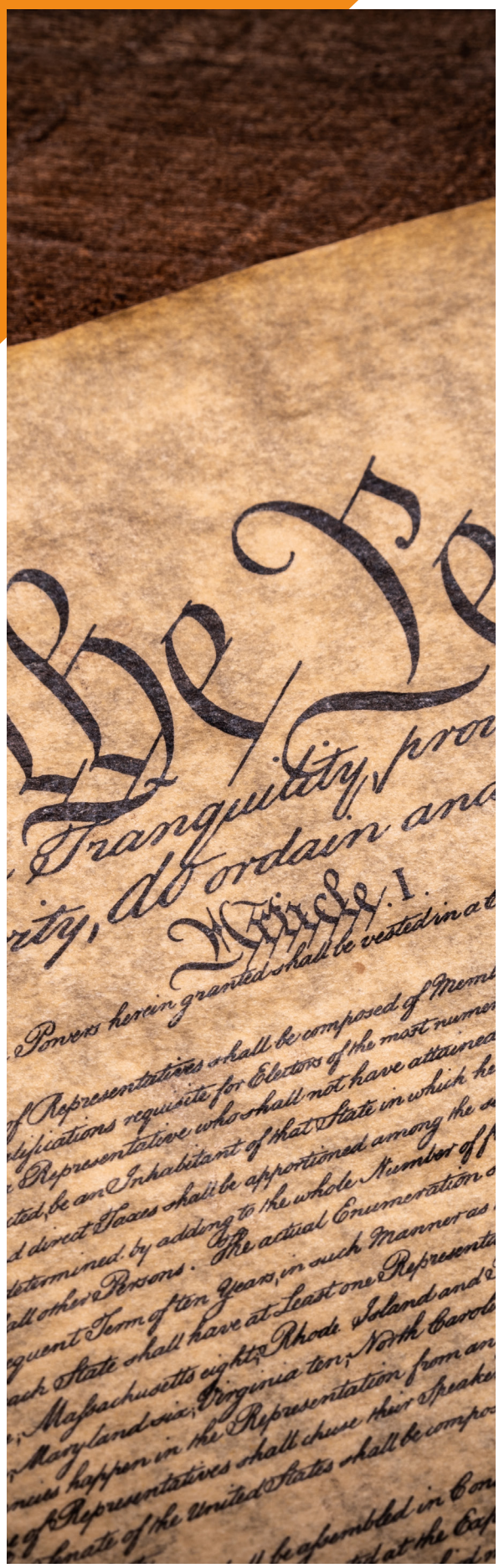
According to Greg Tanaka, "Roughly 1.4 trillion photos are taken a year and increasing, so there is a chance that some low number of innocent person(s) each year will unfortunately get mistakenly ensnared as a child pornographer even for images with no naked children." In other words, due to the sheer volume of images that will be impacted by Apple's CSAM policy, there are bound to be errors.

Matthew Green, one of the top cryptography researchers at Johns Hopkins University, warns of the possibility for the system to be manipulated so as to frame innocent people. According to Green, malicious actors could send seemingly innocuous images to people with the intention of triggering a match for child abuse material. These images could easily fool Apple's algorithm and result in law enforcement being alerted.

Additionally, once the threshold has been reached, the account will be flagged and undergo a human review. Presumably, this human review is to reduce the chance of an account being flagged by mistake. But does the person conducting the review have the legal authority or standing to do so?

Apple has not yet announced the specifics of its human review process. But whether such a review were to be conducted by Apple, NCMEC, or a law enforcement agency, the fact remains that an individual user's possessions would be searched without any reason to believe a crime had been committed. This potential encroachment on Fourth Amendment protections almost certainly outweighs the potential benefits of this new policy.

But What about My Constitutional Rights?



The biggest concern about Apple's new child abuse material policy is one of legality. According to Charlene Collazo Goldfield, an attorney with the U.S. Federal Government, there may be a gap in federal regulations that has not yet reviewed this kind of "seizure" using technology.

Goldfield states, "The Supreme Court determined in Carpenter v. United States that law enforcement needed a warrant to locate information from cell phone sites because of the intricacies and reach of technology, but our legal precedent has not kept up with technological innovation, and so the official act of scrubbing or obtaining social media and public access materials by law enforcement is not necessarily regulated. Not to mention, content moderation standards are determined by the companies themselves."

In other words, Apple may be violating the privacy of its users without any government subpoena. And because there isn't a government subpoena, anyone accused of possessing child abuse material would be left with no way to challenge the search and seizure. It would be one thing if a detective broke into your computer to obtain evidence; it's another when Apple is the one doing it.

Even if the privacy violations aren't enough, there's also the fact that Apple employees are simply not equipped to determine what should or should not be reported to the authorities. Apple's human review process is giving laypeople immense legal power to violate device users' privacy and carry out law enforcement at their own discretion.

Additional questions remain around what could happen once law enforcement is notified. What government agency is responsible for verifying the match? Is an arrest warrant issued immediately or does law enforcement conduct its own review?

Apple has yet to make clear its process for reporting CSAM to the police, and the chain of custody of information is unclear. Without a guaranteed way of ensuring that the user is actually in illegal possession of child abuse material, Apple runs the risk of wrongfully accusing people of having child sexual abuse materials. The possibility that people could be exposed to an improper investigation and have their family and friends interviewed is unacceptable.

One might be inclined to defend Apple's actions by saying that they are simply reporting illegal material obtained as part of a routine review, similar to traffic stops as legal, routine safety checks in which officers pass out literature on drunk driving. But, unlike traffic stops, Apple can't establish that they're innocently scanning and seizing data as a mere consequence of reviewing the device. They have specifically designed and employed software for the sole purpose of invading user privacy.

Data Breaches

Aside from the privacy violations and potential improper flagging of accounts, Apple's new CSAM policy exposes every single iPhone user to the potential of data breaches. We've already talked about the preexisting encryption gaps regarding mail and iMessages that currently put users at risk of having their data leaked. And, although Apple has told us before that data is encrypted end to end, the company has access to iCloud backups which store encryption keys, and therefore the data could easily be decrypted.

This new plan creates cause for concern due to the simple fact that Apple has already suffered numerous notorious data leaks. Just recently, a bug was found in Apple's iOS that automatically ran data within iMessages and attachments. This included messages sent from strangers, which could easily contain malware that puts users at risk. With all of these gaps in security, it's certainly plausible that Apple's new photo-scanning plan could contain similar gaps that would leave its devices vulnerable to attackers.

To enact its new child abuse material policy, Apple must do something it has previously refused to do: create a back door into its devices. But, by creating a back door for company employees to use to monitor and report child abuse material, Apple has created a back door that anyone can potentially hack into and access. The existence of this back door means that criminals will have a new opportunity to access communications and data that should be kept safe.

Who May Be Affected by Apple's New Policy?

Apple's new policy affects far more than just the criminals in possession of child abuse material it purports to target with its new technology. Anyone who has received this kind of image—including, for example, a medical professional treating victims of sex abuse or a lawyer defending a client—is at risk of being falsely accused of possessing child pornography.

"The technology would make it difficult for such professionals to comply with established privacy standards, and could also cause irreparable damage for wrongly reported cases," says Professor Rushdi.

So who exactly could incorrectly fall under the crosshairs of Apple's new policy?

Parents | Images of their children on their phones could be mistakenly flagged.

Any parent with pictures of their child on their phone may be at risk of being incorrectly flagged. Consider, for example, a picture of a mother bathing her toddler.

While undeniably innocuous, this could potentially be mistaken as child sexual abuse materials by an imperfect algorithm. This means that parents, grandparents, family members, and even childcare workers could all be at risk of false flagging.

Who May Be Affected by Apple's New Policy?

Healthcare Providers | Images of their patients could be mistakenly flagged.

Healthcare professionals who could potentially be impacted include:

- Psychiatrists
- Psychologists
- Physicians
- Family and marital therapists
- Social workers
- Professional counselors
- Social workers who work with victims of child abuse

Doctors and pediatric health care providers have the potential to be major unintended targets of Apple's new policy. Not only could they be falsely accused of having child sexual abuse material on their phones, but they could also run into the problem of HIPAA violations. HIPAA has a very strict protocol regarding the privacy of patient data, and Apple's new policy directly puts that data at risk.

"Doctor-patient confidentiality is not voided when communication moves onto electronic/digital/web-connected platforms," states Dr. J. Halpern, a practicing psychiatrist physician whose career includes McLean Hospital and Harvard Medical School. "Medical privacy is afforded the utmost privacy status in the United States. There are likely large forces that would come in to defend a doctor's right to protect the transmission of otherwise 'illegal' material via the internet for purposes of seeking medical attention and care."

Granted, the risk to medical privacy posed by Apple's new policy is narrow in scope. But it does raise a potentially slippery slope regarding evaluations of the health-related data protections currently in place.

"What if this NeuralHash of data is used by healthcare insurance companies to further evaluate insuree risk?" notes Dr. Halpern. "What happens to my patient who sends me a photo of their child who reports they were sexually assaulted? The ability to provide correct private medical counseling, information, and treatment is potentially destroyed by an automatic system that affords no privacy, whether initiated by machine algorithm or human review for contextual validity. I just feel there are tremendous concerns with the wide acceptance of this type of data in which the ground rules for protecting data that is already established as 'sensitive' will be able to remain that way. Because some data is private for a reason."

"What happens to my patient who sends me a photo of their child who reports they were sexually assaulted?"
John H. Halpern, M.D.

Who Else?

Emergency Personnel | Those tasked with protecting children from harm, including firefighters, first responders, law enforcement, and others who respond, report, and defend victims, could be mistakenly flagged.

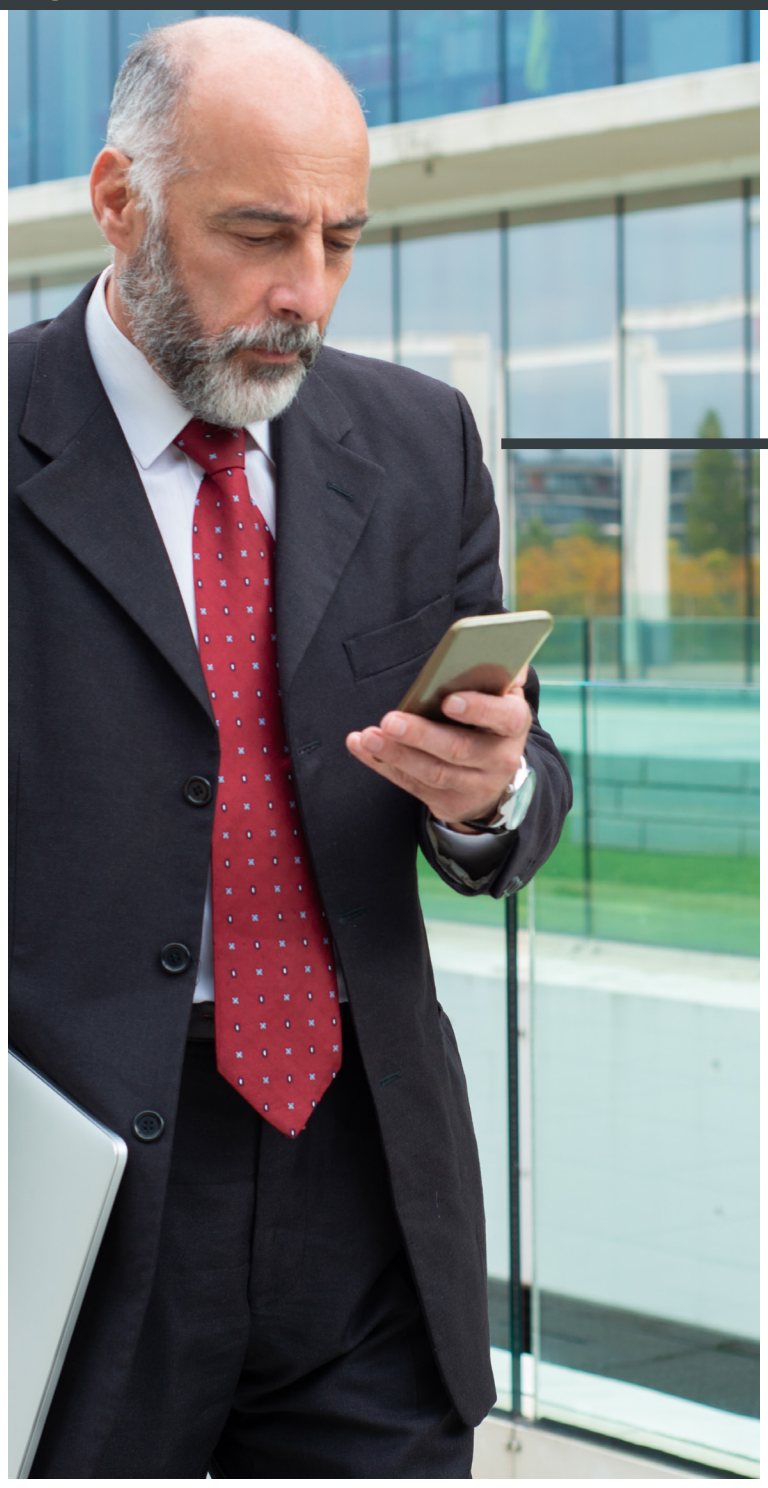
Despite the fact that these professionals are working tirelessly to save lives and combat child sex abuse, under Apple's new policy, they are all at risk of being accused of doing the very thing they're trying so hard to prevent.

Military Personnel

Any military personnel who have encountered child sexual abuse overseas and taken steps to document the abuse with their iPhones could now be at risk.

Researchers/Journalists | Researchers and journalists who are investigating sex offenders victimizing children could be caught in the crosshairs.

Other Government Employees | Any government employee who is indirectly involved with the prosecution or report of child sexual abuse could potentially be affected.



Lawyers

One of the biggest groups with the potential to be accidentally targeted by Apple's new child abuse material policy could be lawyers who are involved with child sexual abuse cases and have received case-related images on their phones. This also includes anyone else involved with these cases, including experts hired by attorneys on behalf of clients, witnesses who are providing evidence of crimes, and even the judges presiding over these cases.

There are many instances, especially in smaller state courts, where attorneys have access to child abuse material images as a part of the prosecution or defense of sex offenders. Not only does this put these lawyers at risk of being flagged for abuse, but it also poses a major issue regarding attorney-client privilege. How can the privileged communications between an attorney and their client remain private when a third party has access to their communications and photos?

Shutterstock

The Future of AI and Your Data

Apple's new policy is certain to bring about a host of concerns with respect to privacy, legal rights, and data leaks. In today's world, cybersecurity is more important than ever, as cybertheft, cyber-trespassing, and hacking are increasingly prevalent. The potential damage caused by the release of personal data or privileged information due to an algorithm error is too great to ignore.

The time to act is now. If you are worried about being ensnared in the crosshairs of Apple's new photo-scanning policy, or about your personal data being breached, you need to act before the new iOS 15 update is released later this year.

Contact the Office of Data Discovery for a consultation to learn more about our services. We help clients protect their images and data from risks such as the risk posed by Apple's CSAM detection technology. Subscribe to stay up to date with the latest developments as we learn more about Apple's new policy, other new technologies, and the risks they pose to your security.