Apple durchsucht iPhones nach Kinderpornografie - Steht man jetzt unter Generalverdacht?

Beitrag von „Prof. Rowan“ vom 18. August 2021, 19:49

Bin vorhin über diesen Artikel: https://www.deutschlandfunkkul...ml?dram:article_id=501710 gestolpert und habe passend dazu ein Video auf YouTube: https://www.youtube.com/watch?v=Drn3hzvv1as gefunden.

Also ich finde das grundlegend bedenklich. Der Zweck heiligt die Mittel...

Ich denke es wird bald so gut wie gar keine Privatsphäre mehr geben, wenn man immer mit "guten Taten" (und bitte versteht mich nicht falsch, Kinderpornografie ist wirklich einer der schlimmsten Dinge im Netz, die alleinige Existenz ist meiner nach ein Armutszeugnis der Menschheit) voranschreitet und meint, dass das die Lösung sei.

Ich finde es erschreckend, dass die Staaten anscheinend ebenfalls machtlos sind. Die Frage die sich mir nun stellt, erst soll es nur die iCloud betreffen, wer garantiert denn, dass nicht permanent mein iPhone durchleuchtet wird? Ist Datenschutz überhaupt noch möglich?

Beitrag von „bounty96“ vom 18. August 2021, 21:01

Sollen sie doch das iPhone durchsuchen. Wer weis ob sie dass nicht eh schon machen. Oder andere Organisationen.

Ich bin mir ziemlich sicher dass das Durchleuchten der eigenen Daten auf anderen Systemen, Geräten, Cloud Anbietern usw.

sowieso schon passiert. Wird halt nur nicht gesagt und kontrollieren kann man es auch nicht.

Ich gehe grundsätzlich davon aus dass sobald etwas Internetzugang hat da nicht nur ich sehen kann was drauf ist.

Wenn ich etwas "sicher" haben will dass niemand anderes es sieht z. B. Bilder dann benutze ich eine Digi Cam ohne WLAN

oder andere Verbindungen und spiele Fotos und Videos einfach auf einen PC der ebenfalls keinen Netzwerkzugang hat.

Und wenn Apple nur auf der Suche nach KiPo, Terrorschei* oder anderem illegalem Zeug ist... finde ich es nichtmal falsch

wenn sie dann damit Leute dranbekommen die in solchen Bereichen mitmischen.

Das was auf den Handys von 0815 normal sterblichen Leuten wie bei mir z. B. drauf interessiert warscheinlich nichtmal

irgend eine KI.

Beitrag von „grt“ vom 18. August 2021, 21:16

hmmmm....

und weil es böse bombenbauer (oder andere schlechte menschen wie dealer, die hochprozentiges vor schulen an kinder verhökern etcpp) gibt, dürften ermittlungsbehörden in zukunft einfach mal so in meine wohnung einsteigen, und alles inzpizieren, was hier so rumsteht? ohne jeglichen anlass, ohne triftigen belegten verdacht, dass ich wirklich gerade daran bin, eine bombe zusammenzulöten, oder mich gerade damit beschäftige den drogennachschub für den schulhof nebenan zu bestellen?

prophylaktisch mal eben meine ganze privatsphäre auf den kopf stellen, meine schubladen durchwühlen, korrespondenzen, notizzettel lesen.... mich also quasi nackt ausziehen, einfach mal so? und das ist ok. weils virtuell ist, nicht wirklich physisch vor meiner nase passiert?

Beitrag von „REVAN“ vom 18. August 2021, 21:25

Niemand durchsucht oder scannt dein lokales Gerät. Der Scan erfolgt nur bei Upload auf die iCloud Server. Wenn du den Foto-Sync einfach beendest, dann wird auch nichts von deinen Bildern gescannt. Der Scan wird – bei Upload – allerdings lokal auf deinem Gerät durchgeführt, liegt einfach daran das X Server exponentiell länger bräuchten, wenn eine Milliarde Bilder zur gleichen Zeit hochgeladen werden würden.

Geht ganz klar aus einem Whitepaper von Apple hervor, wurde bei uns auf dem Discord schon längst besprochen und analysiert.

Beitrag von „bounty96“ vom 18. August 2021, 21:28

Ich glaube nicht dass die einfach nur so aus Lust und Laune jemanden "nackt ausziehen".

Da würden die Ressourcen nicht ausreichen.

Das klingt halt immer so wie wenn die nichts besseres zu tun haben. Aber bevor bei jemandem

eingestiegen wird werden trotzdem erstmal Prüfungen durchgeführt.

Kann schon ab und zu mal passieren dass aufgrund von falschen Verdacht jemand "falsches" durchsucht

wird aber das ist nicht die Regel.

Und wenn die Bock haben sollen sie halt bei mir daheim vorbei kommen und meine Bude auf den Kopf stellen.

Ich müsste zwar danach aufräumen weil wenn sie nichts finden passiert auch nichts weiter und sie gehen wieder

aber mir wärs halt echt egal. Solange das für alle gilt.

Sicherheit > Privatsphäre. Ich bin vermutlich einer von einer Hand voll Menschen die so denken aber mir egal.

Meinetwegen können mich nun alle hassen für diese Meinung. Noch ein weiterer Grund sich über mich aufzuregen:

Ich bin für ein Tempolimit auf der Autobahn. Weil ich glaube dass wenn auch nur 1 Leben dadurch verschont bleibt,

welches sonst durch jemanden mit überhöhter Geschwindigkeit ausgelöscht worden wäre, es die Sache rechtfertigt.

Beitrag von „Bob-Schmu“ vom 18. August 2021, 21:42

> Zitat von bounty96
>
> Ich bin für ein Tempolimit auf der Autobahn. Weil ich glaube dass wenn auch nur 1 Leben dadurch verschont bleibt,
>
> welches sonst durch jemanden mit überhöhter Geschwindigkeit ausgelöscht worden wäre, es die Sache rechtfertigt.

Das hat nichts mit zu viel Tote zu tun, meisten Toten entstehen bei nicht einhalten von Abständen und glaub mir du möchtest keine Kinder aus dem Auto schneiden, das zwischen zwei LKWs zerdrückt wurde, weil der hintere LKW den Abstand nicht eingehalten hat.

Zeig mir eine Autobahn wo man heute noch länger als 10 - 20 Minuten über 200 km/h Fahren kann am Tag, nicht in der Nacht.

Beitrag von „bounty96“ vom 18. August 2021, 21:54

Nein das möchte ich wirklich nicht.

Ich möchte aber auch niemanden "hinten draufhängen haben" der zu schnell aufs Stauende zugefahren ist.

Oder meint er schafft es noch "schnell" vor der Ausfahrt vor mich nur um dann ins Auto zu krachen.

Oder schnell rechts vorbei... Oder auf die AB, vollgas, linke spur und dann voll jemand hinten drauf...

Ja zu wenig Abstand gehört mit dazu aber das eine schließt das andere ja nicht aus.

Und es geht auch nicht darum >10 Minuten 200 oder so zu fahren. Solche Sachen wie oben beschrieben passieren

auch wenn man nur 30 Sekunden 200 oder schneller fährt.

Und nehms mir nicht übel aber dem Motorrad auf deinem Profilbild nach zu urteilen steht das nicht nur bei dir rum

sondern du fährst auch damit.

Ausnahmen bestätigen die Regel aber Motorradfahrer (zumindest 90% von denen die mir begegnen)

sind die größten ******* im Straßenverkehr.

Beitrag von „greecedrummer“ vom 18. August 2021, 23:01

Alles was mit USA Verträgen abgewickelt wurde, unabhängig ob der Standort der Server auf US Boden sei oder nicht, obliegt bei Ausschließung eines Vertrages und deren Nutzungsbedingungen (Einwilligungserklärung bei Installation Software inkludiert) der Regulierungs- und Sicherheitsbehörden und dessen Zugehörigkeit beim FBI und CIA und einige mehr, dass alle Files automatisch gescannt werden, die von großen Anbietern wie Samsung, IBM, Apple, Microsoft. (...) als öffentlichen Speicherort angeboten wird. In der EU läuft es bisschen anders, so zumindest vor den Lichtern.

Hinter den Kulissen wird alles überwacht, Vorreiter ist China. Im Endeffekt, wer nichts zu verbergen hat, hat auch nichts zu befürchten. Wer seine PIN und TAN nicht veröffentlichen will, der uploadet auch diese Daten nicht

Ob es jedoch auf Smartphones usw von Herstellern gescannt wird, bleibt akademisch.

Als Samsung anfangs jede Vorwürfe von sich schütteln wollte, dass gewisse TV Modelle mit fest-integrierten Videokameras und Mikrofonen heimlich und ohne Einwilligung der Nutzer alles aufgenommen hat wen TV online war, brach eine Lawine aus.

Als Edward Joseph bekannt auch als *Edward Snowden* die Welt der Geheimdiensten in den USA und Weltweit ins wanken brachte, hat sich die Welt auch nicht angefangen umgelehrt zu drehen. Geändert hat sich nichts.

Wir werden Tag täglich überwacht, ob und wie es Nutzen oder Schaden haben könnte, lässt man uns "scheinheilig" selbst entscheiden mit etlichen Einwilligungserklärungen. Profan ist es natürlich, dass wir mit nacktem Zeigefinger auf China zeigen. Dieses Model der Gesichtssoftware Erkennung usw läuft seit Jahren in GB und EU! Interpol nutzt es schon seit 2006! Täglich wird der Code verbessert und ausgetauscht. Ob Pornografisches Material oder kryptische Texte auf Server laufen, werden analysiert und ausgewertet. Wie es dann weiter geht, das hängt vom Staat ab.

Beitrag von „Horsti“ vom 19. August 2021, 00:57

Ich bin prinzipiell gegen Überwachung und Aus-Spionage. Wenn dadurch Das Leben für einige besser wird ok aber ich bin immer noch dagegen da es für mich nicht in Relation zum Nutzen steht.

Die Auswertung des Materials was man da findet, findet ja erst mal hiner verrschlossenen Türen statt und selbst wenn es die Beweisumkehr bei uns wohl nicht gibt bleibt immer was hängen.

Bin aber auch zwiegespalten weil ich denke das wir alles Mögliche tuen sollten um die Jüngsten der Gesellschaft zu schützen. Ist halt alles nicht so einfach zu klären irgendwie ist die Welt dann doch nicht Schwarz/Weis

Argumentations-Ketten die das Wort "Autobahn" inne haben würde ich nicht benutzen!

Viel zu oft gehört in Politischen Diskussionen. War immer Falsch und immer Scheiße.

Edit:

Bei Menschen, wo ein begründeter vor Verdacht besteht, sollte es den ermittelnden Behörden dann aber schon gestattet sein genauer hin zu sehen.

Beitrag von „Prof. Rowan“ vom 19. August 2021, 06:43

bounty96 auch wenn man jede Meinung tolerieren muss, ist deine Einstellung meiner Meinung nach die bedenklichste. Wenn einem alles egal ist, alles über sich ergehen lässt und man sich eh damit abfindet, dass einem Unrecht getan wird, dann ist man entweder Masochist, oder einfach nicht in der Lage den Ernst zu verstehen. Das ist meine persönliche Meinung.

Das irgendwo immer irgendwer, ob Firma, Staat, vielleicht auch der Arbeitgeber, Daten abgreift und somit die Privatsphäre verletzt, mag sein.

Aber damit öffentlich zu hausieren unter vorgehaltenem "guten Zweck", naja zerstört mein Vertrauen.

REVAN in Ordnung, auch wenn sich das vorerst auf die iCloud ausschließlich bezieht, bin ich der Ansicht, dass bei einem so eng verwobenen Netz der iOS-Services und Devices, es nicht nur bei den Cloud-Diensten bleiben wird.

Traurig, wenn auch dieses sensible Thema innerhalb von wenigen Tagen wieder bei den meisten in Vergessenheit geraten wird. Mal sehen was in Zukunft noch alles passieren wird.

Beitrag von „REVAN“ vom 19. August 2021, 07:36

Es geht aber erstmal nur um die iCloud + iMessage (bei Kinder-Accounts in der Familienfreigabe) und das auch nur in den USA. Malt doch den Teufel nicht schon vorher an die Wand, der kommt schon früh genug aber noch nicht jetzt.

Deine Fotos und Bilder sind Apple während der Überprüfung nicht bekannt, weil das anhand von irgendwelche kryptischen Hash-Werten verglichen wird.
Du hast eine lokale Datenbank von problematischen Hash-Werten auf deinem Smartphone und

darauf hin werden die Hash Werte deiner Fotos mit den Hash-Werten aus der Datenbank abgeglichen.

Wenn da ein Treffer sein sollte, nennt Apple das Zufall. Auch bei nachfolgend 29 anderer Treffer nennt Apple das immer noch Zufall, wenn du aber 31 + mehr problematische Bilder auf deiner iCloud hast dann schaut sich das Apple mal genauer an und auch nur dann.

Ich verstehe es ja wirklich, dass ihr das alle nicht möchtet. Ich möchte das auch nicht, von daher habe ich meinen iCloud Foto Sync einfach abgeschaltet und gut ist. Ihr dürft auch nicht vergessen, dass die Aktion erstmal mit der DSGVO und dem Datenschutz Konform sein muss, und wenn es das nicht ist würde Apple ja sein Gesicht verlieren. Kann mir nicht vorstellen, dass die wollen das die BRD Strafanzeige stellt.

Wartet doch einfach erstmal ab und macht den Foto Sync aus.

Ich hab auf meinem Smartphone irgendwie 300+ Memes liegen, die können sich die gerne anschauen. Hoffentlich lachen die dann auch mal kräftig. Würde mich freuen.

Ich könnt gar nicht meine ganzen Fotos auf der iCloud speichern, weil ich dann keine Backups mehr machen könnte, bei 5 GB Volumen :*D

Beitrag von „griven“ vom 19. August 2021, 07:46

Spannend wird sein zu sehen wie weit Apple das Spiel in der EU treiben kann/darf bzw. wie schnell die EU die Hosen runter lässt und den eh schon zahnlosen Tiger DSGVO einpackt bzw. gar nicht erst von der Leine lässt denn klar ist ein solch tiefer Eingriff verstößt eindeutig gegen die DSGVO.

Um es ganz klar zu sagen Ich finde es gut das etwas gegen Kinderpornografie unternommen werden soll und ich finde es auch gut das Hersteller von Geräten die die massenhafte Verbreitung solchen Materials ermöglichen das Heft in die Hand nehmen wo die Politik und die Ermittlungsbehörden versagen allerdings nicht mit solchen Mitteln/Maßnahmen und nicht indem man die gesamte Bevölkerung unter Generalverdacht stellt.

Was Apple da technisch plant ist das was technisch machbar ist und das sie es nicht einfach stillschweigend machen sondern öffentlich darüber berichten ehrt sie auf eine gewissen Weise und hebt sie von der großen Masse ab die nämlich ziemlich sicher auch jetzt schon massenhaft

persönliche Daten analysieren und sei es nur zum Zwecke der Werbung. Gerade die großen Player wie Google, Amazon und Co. werden Wege gefunden haben ihre zum großen Teil kostenfreien Cloud Dienste durch die Nutzung der vom Nutzer freiwillig in die Cloud gelieferten Daten zu vergolden.

Das eigentliche Problem an Apples Ansatz ist daher meiner Meinung auch nicht das aufspüren von Kinderpornos damit hätten vermutlich die wenigsten wirklich ein Problem das eigentliche Problem liegt darin das diese Techniken auch ganz gezielt für andere Dinge genutzt werden können. Durch das etablieren einer solchen Möglichkeit/Technik schafft man Begehrlichkeiten die dann auch ausgenutzt werden. Hat man die Tür einmal aufgestoßen ist es halt schwer bis unmöglich unerwünschte "Besucher" draußen zu halten. Die Gefahr besteht also das der, eigentlich gut gemeinte, "Dienst" missbraucht wird um zum Beispiel regierungskritische Organisationen aufzuspüren (in Ländern wo das ein Regime keine Kritik duldet). Natürlich tönt Apple jetzt das so etwas nicht passieren wird aber am langen Ende ist auch Apple nur ein wirtschaftlich agierendes Unternehmen und spätestens dann wenn Ihnen in Schlüsselmärkten die Zulassung ihrer Geräte verweigert wird wenn nicht gewisse "Spionage" Dienste eingebaut werden wird auch Apple einknicken.

Beitrag von „Sascha_77“ vom 19. August 2021, 07:47

Prof. Rowan

Sehe das ähnlich wie Du. Wie oft habe ich das Argument schon gehört: "Och, ich hab doch nix zu verbergen". Die Sorglosigkeit dieses Thema betreffend ist schon irgendwie erschreckend. Ich bin jetzt sicher alles andere als ein Paranoiker aber Clouds für meine **persönlichen Daten** bei irgendwelchen Anbietern habe ich noch nie betreten. Ich hoste meine Dienste und Daten stets alles selber. Klar könnte man jetzt sagen: "Aber was ist wenn die NSA im Debian Betriebssystem eine Backdoor eingebaut hat?". 100% sicher kann man nie sein. Aber wenn es danach ginge dann müsste man alles abschaffen und wieder im Mittelalter leben. Das kann auch nicht das Ziel sein. Ist halt wie im echten Leben draußen, ein gewisses Risiko gibts immer.

Zumindest kann ich für mich sagen, dass ich, soweit es mir möglich ist, meine Daten vor fremden Zugriff schütze. Sollte dennoch sich jemand Zugang verschaffen ist das zutiefst verwerflich aber ändern kann man es dann leider nicht. Aber das ich von Hause aus Tür und Tor bereitwillig "öffne" und mir es egal ist ... ne eher friert die Hölle zu.

EDIT:

So Sachen wie Smartphone generell sind da eh schon "schlimm" genug. Da trägt man im Grunde schon ein prima Einfallstor mit sich tagtäglich herum. Erschreckend fand ich letztens einen Beitrag vom CC2 Tv. Durch das Mikrofon kann man mittels bestimmter Tonfrequenzen Befehle auf dem Handy ausführen bzw. Apps ansprechen. Gucke ich also Fernsehen und da wird eine fürs Menschliche Ohr unhörbare Frequenz ausgegeben und das Handy ist auf Standby (was sicher bei 99% der Leute der Fall sein dürfte) kann das Handy unbemerkt irgendwelche Sachen ausführen. Remote Control sozusagen. Im harmlosesten Fall könnte man also rausfinden was derjenige in dieser Sekunde gerade auf dem Fernsehen schaut. Die Möglichkeiten die generell durch so ein Vorgehen möglich sind sind schier endlos. Immerhin könnte man das durch einen kleinen Störsender unterbinden (oder natürlich das Handy runterzufahren). Aber wer kommt schon drauf sich sowas ins Wohnzimmer zu legen.

Beitrag von „REVAN“ vom 19. August 2021, 07:54

griven

Das der Punkt - wie immer hast du den Nagel auf den Kopf getroffen. Wofür könnte man das System noch benutzen? Btw. damit Apple in China die iCloud anbieten kann, werden die Daten bei einem Chinesischen Unternehmen gehostet, also ja - du hast recht.

Auch könnten Bilder so Manipuliert sein, dass das harmlose Reddit Bild dir mächtig Probleme bereiten kann.

Ich glaube weniger, dass das System von Dritten großartig ausgenutzt werden kann um damit Schaden anzurichten, und wenn dann kann man sich Gedanken machen.

Geht ja wirklich erstmal nur um Kinderpornographisches Material. Sehr viele Zeitungen und Online-Medien haben da in den letzten Tagen mehr Clickbait draus gemacht, als es ist.
Von daher verweise ich nochmal auf das Whitepaper von Apple selbst, damit man den Vorgang besser verstehen.
Die lokalen Bilder - die nicht in der iCloud sind - interessieren dabei gar nicht, weil wenn es so wäre dann wäre das ein harter Eingriff in den persönlichen Lebensbereich und somit in keinem Land umsetzbar (gut in ein paar vielleicht, aber nicht in DE und den USA).

Beitrag von „pebbly“ vom 19. August 2021, 08:12

Ich bin erstaunt wie wenig technisches Verständnis zu der Problematik hier doch herrscht. Es scheint, als ist den wenigsten die Tragweite eines so etablierten Systems bewusst!

> Zitat von griven
>
> das eigentliche Problem liegt darin das **diese Techniken auch ganz gezielt für andere Dinge genutzt werden können**. Durch das etablieren einer solchen Möglichkeit/Technik schafft man Begehrlichkeiten die dann auch **ausgenutzt werden** . Hat man die Tür einmal aufgestoßen ist es halt schwer bis unmöglich unerwünschte "Besucher" draußen zu halten. Die Gefahr besteht also das der, eigentlich gut gemeinte, "Dienst" missbraucht wird um zum Beispiel **regierungskritische Organisationen aufzuspüren** (in Ländern wo das ein Regime keine Kritik duldet). Natürlich tönt Apple jetzt das so etwas nicht passieren wird aber am langen Ende ist auch Apple nur ein wirtschaftlich agierendes Unternehmen und **spätestens dann wenn Ihnen in Schlüsselmärkten die Zulassung ihrer Geräte verweigert wird wenn nicht gewisse "Spionage" Dienste eingebaut werden wird auch Apple einknicken**.

Griven hat das gut gesagt, so dass ich die relevanten Teile hervorheben möchte (ich hoffe das ist okay?).

- Schaut man sich Apples verhalten in **China** an, ist es **keine Frage ob, sondern wann** sie einknicken werden. Denn sie **sind schon mal eingeknickt**, Stichwort VPN und iCloud in China.

- Viel Gefährlicher hierbei ist, dass nun Feinde von Regimen einfach auf der **ganzen Welt** gesucht werden, 1984 lässt grüßen

- Die Hashs scheinen technische Probleme zu machen, da unterschiedliche CPUs unterschiedliche Hashs generieren: https://twitter.com/OmerK/status/1427935805956317186

- Unterschiedliche Bilder können trotzdem den gleichen Hash generieren: https://twitter.com/SarahJamie…tatus/1428082934393688066

- **Es gibt keine technische Lösung für ein soziales Problem!**

- Es widerspricht einfach sowas von Apples Werbung zum Datenschutz

---

Beitrag von „mhaeuser“ vom 19. August 2021, 08:15

Ich habe langsam keinen Nerv mehr, den Klick-geilen "Medien" und ihren "Experten" hinterherzukehren. Daher wünsche ich viel Spaß mit weniger technischem Hintergrund und mehr Sarkasmus. Manche sollten ein bisschen mehr auf ihre Daten Acht geben, und manche, was sie ungefiltert von Schundseiten wie heise übernehmen.

Jeder normale Cloud-Anbieter scannt die Daten in der Cloud. Die liegen dort, genau wie bei Apple, ja freudig ohne E2E herum. (Wer Cloud-Anbieter ohne E2E nutzt, macht sich sowieso ein wenig lächerlich, aufzuschreien, wenn die Daten in irgendeiner Form angerührt werden.) Dort läuft dann eine KI auf den Rohdaten und, wenn (Kriterien oft intransparent) die KI meint, unangenehmes Material zu sehen, wird das Konto geschlossen. Im Falle von Microsoft teils ohne Möglichkeit der Richtigstellung. Das Foto deines eigenen Kindes in der Wanne ist gar kein Kinderporno? Schade, deine XBOX-Spiele kassieren wir trotzdem ein. Kein Grund zum Aufschrei, Leute, das hat alles seine Richtigkeit.

Wieso sollte Apple also etwas anders machen als alle anderen? Weil die Nazis hinter'm Mond unsere Daten wollen, oder? Ja klar, aber andere Gründe gibt es als Schein trotzdem noch. Der Scan auf dem Gerät erlaubt es Apple so zu tun, als müssten sie die Daten niemals anrühren. Dort wird nämlich ein Hash der (noch!, sie kommen ja alle in die iCloud) lokalen Daten generiert (von einem Hash kann man niemals eindeutig auf eine Ursprungsdatei zurückrechnen) und mit einer Datenbank aus Hashes von Kinderpornos verglichen. Die KI wird also von "ist das ein Kinderporno?" reduziert zu "ist das ein Kinderporno aus der Datenbank?" Bei 30+ Übereinstimmungen schaut Apple sich das Konto an. Frech, oder? Die schauen sich dann die Daten an, statt einfach das Konto für immer wegzusperren. Im Namen des Datenschutzes sollten sie das tun, und direkt die Behörden alarmieren, oder?

Irgendwann kommen wir an den Punkt, an dem ich gefragt werden: Hey Fritz, das sieht doch bisher alles fast so aus, wie bei anderen normalen Cloud-Anbietern, oder? Da ist ja auch nichts E2E und die lassen ja auch KIs laufen, sogar auf den Rohdaten. Apples Methode klingt doch durch die Hash-Geschichte eigentlich sogar privater, oder? Ja, soll ja auch gut klingen, denn direkt nach dem Hash-Check bekommen die Nazis hinter'm Mond eure abfotografierte TAN-Liste. Bei anderen Cloud-Anbietern hätte das nicht passieren können.

Und dann kommen bald bestimmt wieder die Datenschutz- und Sicherheitsexperten "Ladida, die Datenbank könnte Materialien politischer Feinde enthalten, oder jemand könnte dir Collision-Bilder zuschieben". Welch Offenbarung, wahre meister ihrer Kunst, solch neue und

kreative Ansätze würden bei den KI-Ansätzen der Konkurrenz natürlich nicht funktionieren. Ahem.

Beitrag von „REVAN“ vom 19. August 2021, 08:26

Genau das ist das Problem - und nichts anderes: Die absolute Fehlkommunikation in den Medien und die Meinung von irgendwelchen Leuten, die sich selbst als „Experte“ bezeichnen. Sicherlich mag es da einige fundierte Aussagen dazu geben, aber oftmals ist das einfach Kram ohne Quelle. Eine kritische Denkweise täte dem Thema mal ganz gut, und damit meine ich nicht die Vorgehensweise von Apple.

Bisher war das ja aber immer schon so, dass erstmal alles schlecht geredet worden ist was Apple neu einführt und andere schon seit Jahren praktizieren.

mhaeuser - absolutes Top Kommentar: +1

Beitrag von „talkinghead“ vom 19. August 2021, 08:48

Irgendwie kann ich Apple etwas verstehen.

Die ganzen “nützlichen” Features, die u.a. in der Photo App stecken wie Personenerkennung, Motiverkennung, Jugendschutz usw. werden(müssen) während der Entwicklung getestet werden.

Ich will jetzt nicht behaupten, dass Apple ihre Entwicklungstest wahllos mit beliebigen Bildern in der iCloud ausführt, vielleicht hab ich in den AGBs sogar irgendwo da zugestimmt. Jedenfalls, wenn ich dort Entwickler wäre und würde hypothetisch auf solche Bilder stoßen - vielleicht nur weil man einen Nacktfilter testen sollte, in guter Absicht, um jedem Einzelnen dabei zu helfen, dass seine selbst erstellten Nacktbilder etwas sicherer auf dem iPhone verbleiben und nicht gesynct werden - wie gesagt, alles nur hypothetisch - wenn ich dann dabei auf Kinderpornbilder stoßen würde, könnte ich nicht einfach sagen “da kann man nix machen. Neutralität und Privacy first”. Wenn ich davon Kenntnis genommen hätte und hier die Chance sehen würde, zu helfen, Kriminellen das Handwerk zu legen, Sch*** drauf, dann würd ich das machen. Es hat doch dort eh niemand die Zeit, sich die ganzen anderen Bilder anzusehen und

dann noch die Zeit zu investieren, die in einen persönlichen Kontext zu stellen.

Das ganze tue ich für mich nicht mit “ist doch kein Problem” ab, sondern bringt mich zu einer erneuten Risikobewertung der Technologie, was ich ihr anvertrauen will.

So wie man das bisher auch permanent machen musste. Auf den Offline Computer der pre Internetzeit konnte man gecrackte Sachen bedenkenlos laufen lassen. In der Always - Connected Zeit würde das nicht mehr machen. Is halt so.

Beitrag von „umax1980“ vom 19. August 2021, 08:50

Letztlich haben die jeweiligen Smartphone Hersteller durch Touch- und danach Face-ID oder wie die Technik jeweils bezeichnet wird, so viele verwertbare Daten bekommen. Da kann man doch eine saubere Datenbank aufbauen und an belebten Plätzen weiß man dann wer sich dort aufhält.

Geändert werden wird es nicht mehr, man kann diesen Verlauf weder bremsen oder gar aufhalten.

Wenn ich für mich selber spreche, meine wichtigen Daten sind für mich unterwegs nicht greifbar. Alles wichtige ist für mich nur „at Home“ erreichbar. Cloud-Dienste nutze ich nicht.

Interessant ist in diesem Zusammenhang auch die DSGVO, mal sehen wie stark dieses wirklich ist….

Beitrag von „mhaeuser“ vom 19. August 2021, 10:44

Klar, die Personen, die Face ID nutzen, sind sonst komplette Geister und man kommt kaum anders an Fotos von ihnen. Clever, Apple, clever. Wer von denen hat schon Zeit für eine PIN...

Beitrag von „Sascha_77“ vom 19. August 2021, 10:57

> Zitat von Download-Fritz
>
> ...Wer von denen hat schon Zeit für eine PIN...

Genau das ist das. Der Mensch ist ja von Natur aus eher "faul" bei so etwas. Wobei ich zugegebenermaßen bei meinem Android den Fingerabrucksensor nutze. Aber nicht in der Hauptsache wegen Entsperren sondern wegen der Apps um nicht überall dort das Passwort von Hand eintippen zu müssen. Hätte ich die Möglichkeit von Face-ID würde ich trotzdem maximal beim Fingerabdruck bleiben.

Ein etwas erschreckendes Beispiel ist eine meiner beiden Schwestern. Sie ist wirklich handysüchtig und kann das Ding keine 2 Sekunden aus den Augen lassen und lebt einen Großteil des Tages in der virtuellen Welt. Dann in ihrem Haus noch ein paar Dot´s verteilt. Sie ist der Traum eines jeden Datensammlers. Und ich glaube von solchen Menschen gibt's einige.

Beitrag von „mhaeuser“ vom 19. August 2021, 11:16

Sascha_77 Das war sarkastisch gemeint im Sinne, dass, wenn jemand sich anonymisieren will, die Person garantiert nicht Face-ID nutzt und, wenn sie es nicht will, es genug andere Quellen gibt. Face-ID macht die """Spionage""" nicht einfacher, genau wie es CSAM nicht tut. Gibt viel einfachere Wege ans Ziel zu kommen.

Recht hast du unabhängig davon trotzdem.

Beitrag von „umax1980“ vom 19. August 2021, 11:54

Hier ist doch die Rede von den Abermillionen an gut gescannten biometrischen Daten, die kann man so gut nutzen. Ich hatte im vergangenen Jahr ein Online-Meeting bezüglich Marketing und dessen Einsatzgebiete in digitaler Form. Einige Unternehmen sind in diesem Bereich dermaßen weit, und welche Möglichkeiten da noch drinstecken - wirklich interessant

und dennoch erschreckend.

Beitrag von „ozw00d“ vom 19. August 2021, 12:14

Ich kann diesen Aufschrei in den Medien nicht verstehen.

Wovor hat man Angst?

Wie mhaeuser schon schrieb, geht es hier nicht um ein Foto des eigenen Kindes in der Badewanne.

Dahinter stehen Algorithmen und wie Fritz schrieb gewisse Datenbanken.

Selbst die beste KI gestützte suche ist aktuell noch nicht in der Lage das einwandfrei zu filtern.

Ich sehe das auf der einen Seite sehr positiv, der Kinderpornografie muss einhält geboten und die Menschen die solche Abscheuliche taten begehen, einhalt geboten werden.

Leider sind die Gesetze in diese Richtung derart Lasch, das man eigentlich nur im Dreieck Kotzen möchte.

Bedenkt man was einem eine Raubkopie einbringen kann und vergleicht man eine solche Grausame Tat damit.

Naja wie auch immer, wer nichts zu verbergen hat, der braucht sich m.E. auch nicht in die Hose machen.

Angst vor der Justiz hat nur der, der auch etwas zu verbergen hat.

Apple, MS und co. Scannen die Daten so oder so.

Welche Cloud ist da völlig egal.

Eine DSGVO sollte nicht vor dem Gesetz in der Richtung stehen das solche Menschen dingfest gemacht werden.

Mir ist es daher ziemlich egal was die von mir scannen.

Glaubt ihr ernsthaft das der Staat hier einen Riegel vorschiebt? Ich denke nicht, schaut mal in Richtung sogenannter Staatstrojaner, was ein leichtes den Datenstrom abzufangen und jemandem etwas unterzujubeln wovon der Nutzer ausgeht das sei legitim.

Oder Ping SMS.

Die technischen Möglichkeiten des Staates sind da nahezu grenzenlos.

Und der Staat soll jetzt etwas gegen Apples Idee unternehmen? Lächerlich, die reichen sich die Hände und ich hab nichts dagegen.

Beitrag von „mhaeuser“ vom 19. August 2021, 14:07

umax1980 Face-ID-Daten verlassen das Gerät nicht. Wenn du die unfundierte Hypothese aufstellst, dass sie es doch tun, braucht es einen Grund. Dein Grund ist "Leute an Orten zu erkennen". Leute an Orten zu erkennen kann man viel einfacher umsetzen, da braucht es keine Biometrie. In den allermeisten Fällen würde die GPS-Funktion des Handys der Betroffenen reichen. Ist das aus irgendeinem Grund nicht möglich, reichen für rudimentäre Erkennung auch Social-Media-Bilder oder dergleichen. Biometrie braucht man dafür in keinem Fall.

Du nimmst realistische Konzepte (Sammlung von Daten aus diversen Quellen) und schwurbelst dir damit unbegründeten Stuss zusammen (Nutzung von biometrischen Daten zur Ortsüberwachung). Und ich will jetzt nicht 50 weitere zurechtgesponnene Gedankenmonster hören, was man mit den Daten alles machen kann, sondern höchstens belegt nachvollziehbare, problematische Dinge.

Beitrag von „griven“ vom 19. August 2021, 14:38

Standortbestimmung geht bei Mobiltelefonen noch viel einfacher dazu braucht es nichtmal GPS

und am langen Ende nichtmal eine aktive SIM im Handy. Ein Mobilfunkanbieter, in dessen Netz sich ein Handy technisch Einbuchen könnte, kann jederzeit, vorausgesetzt das Gerät ist eingeschaltet, bis auf wenige Meter genau sagen wo sich das Gerät befindet. Jedes auf dem Markt befindliche Handy hat zumindest in der Theorie eine eindeutige Kennung an der es im Netz identifizierbar ist (IMEI Nummer) zusammen mit einer SIM Karte wird daraus die IMSI (International Mobile Subscriber Identity) und die ist schon ziemlich eindeutig einer Person zuzuordnen. Die eigentliche Bestimmung des Standorts leistet hier das Mobilfunknetz selbst denn im Netz lässt sich mit sehr geringen Aufwand anhand der HLR Daten bestimmen wo sich ein Handy gerade befindet. Es ist schon so wie mhaeuser ganz richtig schreibt wenn es darum geht Bewegungsprofile zu erstellen sind alle Wege die dazu biometrische Daten verwenden viel zu kompliziert und aufwendig hier kommt man mit sehr viel weniger Aufwand zum Ziel. Aber irgendwie weicht das ja nun vom eigentlichen Thema des Threads schon ziemlich ab 😉

Beitrag von „mhaeuser“ vom 19. August 2021, 14:47

> Zitat von griven
>
> Aber irgendwie weicht das ja nun vom eigentlichen Thema des Threads schon ziemlich ab 😉

Nicht wirklich, ist das selbe Prinzip. Zur """Überwachung""" der Daten braucht es kein CSAM (Face-ID), dafür reicht der nicht-E2E-Speicher (GPS, Netz). Apple kann seit Einführung der iCloud alle Daten dort einsehen, warum sollten sie dafür CSAM einführen? Klar, um alles auf dem Gerät zu überwachen statt nur die iCloud. Wird bestimmt vielfach belegt werden.

Beitrag von „HAI“ vom 19. August 2021, 18:02

Zum Thema, wenn es um privacy, freie Rede und Innovation geht, ist und bleibt hier die erste Anlaufstelle. Es wird keine bessere geben.

Es wird hier selbstverständlich auch Apple analysiert (auseinander genommen) und objektiv bewertet.

https://www.eff.org/

The leading nonprofit defending digital privacy, free speech, and innovation.

Ich denke, wir sind alle der Meinung, daß es, wenn es speziell um die Kinder geht: no mercy und alle "Mittel". Jetzt bleibt dann """nur""" noch Frage nach dem "Mittel". Um eine Antwort auf genau diese Frage drücke ich mich, weil ich sie nicht beantworten kann. s.u.

Beitrag von „cobanramo“ vom 19. August 2021, 19:17

Aus praktischen und Pandemie bedingten Sicherheit hab ich vorhin meinen neugeborenen fotografiert und über iMessage die Hebamme zukommen lassen, die hilft mir dann auch zu entscheiden ob mein Baby an dem sogenannten "Gelbsucht" leidet damit ich reagieren kann.

Ich denke nicht das das Apple interessiert, glaube auch nicht das es verfolgt wird.
Es gibt schon genug böses auf dieser Welt und Gott sei dank wird auch vieles dagegen unternommen.

Man kann auch übertreiben und jedesmal immer wieder den Teufel an die Wand malen.

Klar sollten wir wachsam sein aber bei jedem Blödsinn sollten wir auch nicht showstopper spielen denke ich.

Gruss Coban

Beitrag von „REVAN“ vom 19. August 2021, 19:55

cobanramo

Glückwunsch. Alles gute und wenns das erste ist, wird das zweite nicht so anstrengend 😉

Das ist der Punkt, das Foto ist ja nicht in der Datenbank gelistet, von daher interessiert es auch keinen. Wobei das Feature eh noch nicht ist.

Beitrag von „kaneske“ vom 19. August 2021, 20:38

Wenn ich 10 mal mehr Werbung sehe für 10 Typen die damit erwischt werden nehm ich noch eine Potenz mehr Werbung in Kauf um diese Technik zu tolerieren.

Auslöser ist nicht die Gier, es ist die Verschattung der Straftat in der Anonymität.

Das gilt es aufzuhalten, Freiheit ja ist gerne gesehen.

Aber den Otto Katalog gibt es halt nicht mehr, Vorwerk kommt nicht mehr vorbei und Bofrost Bimmel nicht bei uns.

Ich sehe mehr Vorteile als Nachteile in der Vernetzung.

Ja ich habe nichts zu verbergen und mir ist es egal, was wollen die Jenigen denn tun? Mir meinen Erstwelt Luxus nehmen?

Beitrag von „mhaeuser“ vom 19. August 2021, 20:42

> Zitat von __.__
>
> Es wird hier selbstverständlich auch Apple analysiert (auseinander genommen) und objektiv bewertet.

Ich weiß nicht, was du gelesen hast, aber ich lese hier "mir doch egal, wie privat die Lösung gestaltet ist, es ist nicht maximal privat".

> Zitat

> Again, the bottom line here is that whatever privacy and security aspects are in the technical details, all photos uploaded to iCloud will be scanned.

Sehr, sehr viel Text grundlos über drei Seiten verstreut für weitgehend Nullaussagen. Apples Lösung ist privater als z.B. Microsofts, aber das interessiert natürlich niemanden. Was sich jeder Mal fragen sollte ist, warum Apple in sowas so viel Zeit investiert, und warum eine solche Suche bei den großen Anbietern Standard ist. Wenn gewisse Instanzen bitten, dann ist das keine Bitte, und es gibt nur noch die Schadensbegrenzung.