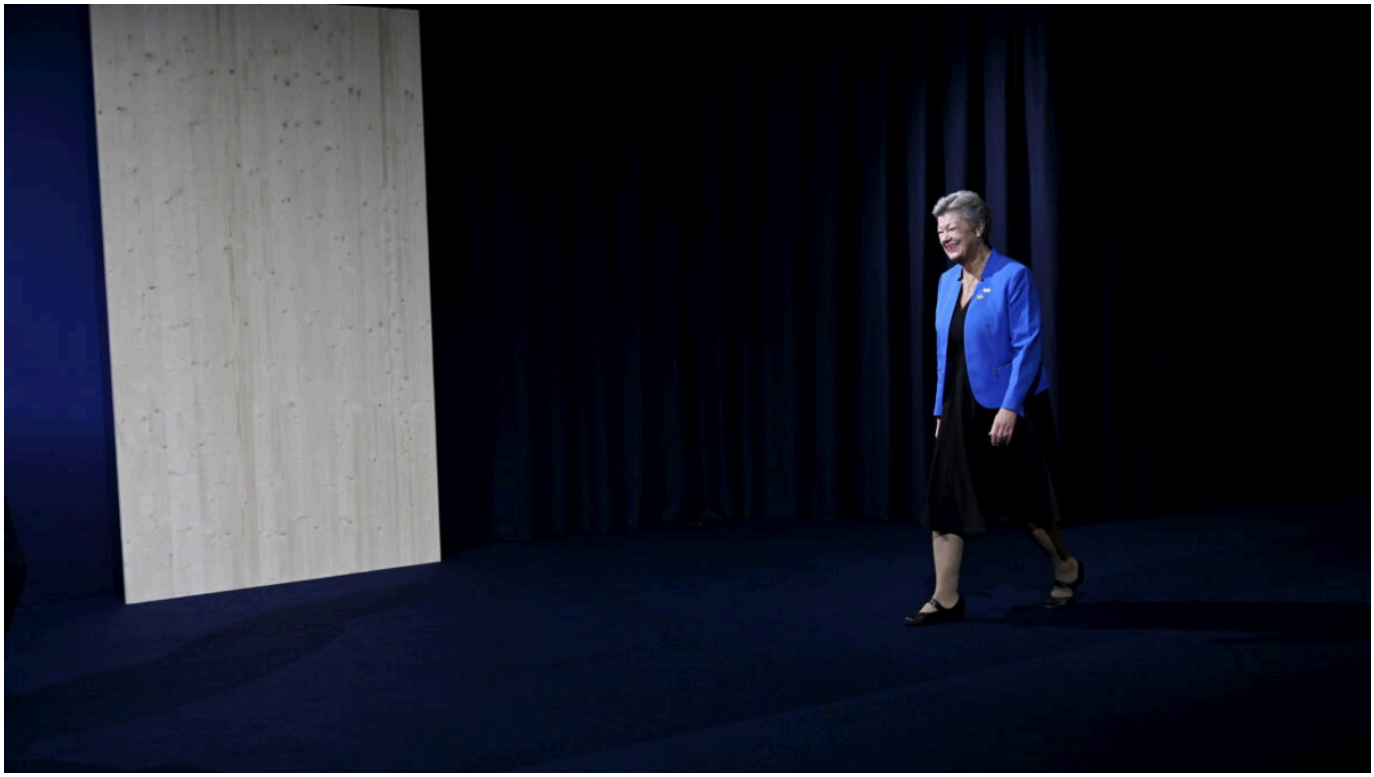
Chatkontrolle

Es ging immer darum, Verschlüsselung zu umgehen

Eine Gruppe von Expert:innen hat für die EU-Kommission Vorschläge erarbeitet, wie sich eine Chatkontrolle technisch umsetzen ließe. Dabei setzen die Vorschläge vor allem auf das so genannte Client-Side-Scanning, aber auch andere Formen der Überwachung verschlüsselter Kommunikation werden angedacht.

16.11.2023 um 12:15 Uhr - Tomas Rudl - in Überwachung - 14 Ergänzungen



EU-Innenkommissarin Ylva Johansson will die Chatkontrolle durchboxen. (Symbolbild)
– Alle Rechte vorbehalten IMAGO / TT

Die sogenannte Chatkontrolle könnte womöglich nur ein erster Schritt sein, mit der die EU-Kommission stückweise verschlüsselte Kommunikation anzugreifen versucht.

Langfristig könnten etwa zwischengeschaltete Server in die Inhalte von Nachrichten hineinschauen, um Darstellungen von Kindesmissbrauch oder sonstige illegale Inhalte aufzuspüren. Das geht aus Empfehlungen hervor, die eine Gruppe von Expert:innen im Rahmen des „EU Internet Forums" für die EU-Kommission erarbeitet hatte.

Letzte Woche war bekannt geworden, dass die EU-Kommission sich sehr einseitig für ihre technische Folgenabschätzung zu dem umstrittenen Chatkotrolle-Gesetzentwurf hat beraten lassen. Den Entwurf hat EU-Innenkommissarin Ylva Johansson vor über einem Jahr vorgelegt, er richtet sich unter anderem gegen die Verbreitung von Missbrauchsinhalten über das Internet, könnte aber einer anlasslosen Überwachung auch anderer Inhalte Tür und Tor öffnen.

Besonders brisant ist an dem Vorschlag, gegebenenfalls auch private Nachrichten zu durchleuchten, die eigentlich mit Ende-zu-Ende-Verschlüsselung gesichert sind. Eine Technik dafür ist als „Client-Side-Scanning" (CSS) bekannt und gleicht Inhalte mit Datenbanken ab, bevor sie verschlüsselt und versandt werden.

Das Vorhaben der EU-Kommission stand von Beginn an unter starker und bemerkenswert breiter Kritik, da damit eine neue Form anlassloser Massenüberwachung eingeführt und zugleich Verschlüsselung geschwächt würde. Kürzlich hat sich das EU-Parlament dagegen ausgesprochen, während sich die EU-Länder noch nicht auf eine gemeinsame Position einigen konnten.

Expert:innen mit Schlagseite

Im Vorfeld hatte sich die EU-Kommission von über 30 Personen beraten lassen. Wie netzpolitik.org letzte Woche berichtete, hatte die Gruppe eine klare Schlagseite: Neben Vertreter:innen von Geheimdiensten und Polizeien hörte Johansson vor allem Expert:innen an, die mit Massenüberwachung nicht auf Kriegsfuß zu stehen scheinen.

Nach unserer Veröffentlichung wurde uns das gesamte Dokument zugespielt, das wir im Volltext veröffentlichen. Darüber hatte bereits Politico im Jahr 2020 berichtet, dem damals veröffentlichten Dokument fehlte jedoch die Liste der Expert:innen. Das undatierte Diskussionspapier gewährt auf 28 Seiten einen Einblick in die Denkweise der Kommission und welche Handlungsoptionen sie überhaupt in Betracht zieht.

EU-Kommission gibt Ziel klar vor

Von Anfang an ist klar: Es geht um die „proaktive Erkennung durch Unternehmen von Bildern, Videos und Text-basiertem Kindesmissbrauch wie Grooming oder Sextortion".

Unter Grooming versteht man die Kontaktanbahnung Erwachsener zu Minderjährigen, Sextortion ist eine Form sexueller Erpressung. Das Papier beschränkt sich auf die Untersuchung von Messenger-Diensten und auf eine „spezifische Art illegaler Inhalte, auf Kindesmissbrauch".

Der Fokus auf derartiges Material erkläre sich unter anderem daraus, dass als solche erkannte Inhalte „unabhängig vom Kontext" seien, anders als etwa mutmaßlich terroristische Inhalte, heißt es in der Einleitung. Das ist eine bemerkenswerte Aussage, schließlich handelt es sich bei vielen Tatverdächtigen um Minderjährige oder um sonstige Nutzer:innen, die aus völlig unverfänglichen Gründen ins Visier von Online-Diensten und Polizeien geraten. Kontext, den automatisierte Werkzeuge nicht erfassen können, ist auch hier entscheidend.

Hauptproblem Verschlüsselung

Das Papier bewertet denkbare Ansätze nach fünf Kriterien: Effektivität, Machbarkeit, Privatsphäre, Sicherheit und Transparenz. Als Hauptproblem verortet es Ende-zu-Ende-verschlüsselte Kommunikation, die führende Messenger-Dienste wie Signal, WhatsApp oder iMessage seit geraumer Zeit standardmäßig einsetzen. „Gibt es irgendwelche technischen Lösungen, die die Erkennung von Missbrauchsmaterial erlauben, während sie die gleichen oder vergleichbaren Vorteile von Verschlüsselung beibehalten?", fragen die Autor:innen.

Aus Sicht hunderter Wissenschaftler:innen und IT-Expert:innen fällt die Antwort darauf nicht schwer: Techniken wie CSS würden Ende-zu-Ende-Verschlüsselung und damit die Privatsphäre schwächen, der Abgleich mit Datenbanken voller digitaler Fingerabdrücke („Hashes") sei manipulierbar und nicht zuverlässig, und automatisierte Erkennung sowie damit verbundene Fehlerraten würden unnötig Ressourcen binden, die dann dem tatsächlichen Kampf gegen Kindesmissbrauch fehlen würden.

Solche Stimmen wollte die Kommission aber augenscheinlich nicht hören oder sie wurden im Bericht nicht merklich gewürdigt – so ist nicht auszuschließen, dass beispielsweise Facebooks Ex-Sicherheitschef oder manche Vertreter:innen von Google oder Microsoft, die mit am Tisch saßen, das Vorhaben kritisch sehen. Sie vertretende Wirtschaftsverbände wie CCIA oder Eco stellen sich nicht von ungefähr konsequent gegen die Aushöhlung von Verschlüsselung.

Bericht ermittelt „Top 3“-Ansätze

Der Bericht listet knapp ein Dutzend technisch denkbarer Ansätze auf, sie reichen vom Status Quo über Inhalteerkennung auf den Geräten beziehungsweise Servern bis hin zu relativ neuartigen Techniken wie der selektiven Überwindung sogenannter homomorpher Verschlüsselung. Einige davon, etwa letztgenannte Technik, würden noch mehr Forschung benötigen, heißt es in der Zusammenfassung. Andere Ansätze wie uneingeschränkte Ende-zu-Ende-Verschlüsselung wie bisher seien für die Lösung des Problems nicht anwendbar.

Als „Top 3“-Ansätze gelten dem Papier zufolge: Inhalte werden vor ihrer Verschlüsselung auf den Geräten der Nutzer:innen in Hashes umgerechnet, während danach ein Server die Hashes mit einer Datenbank bereits gemeldeter Inhalte abgleicht. Das entspricht praktisch dem CSS-Ansatz. Zweitens in Frage käme eine ähnliche Technik, bei der die Hashes teils auf den Geräten selbst und teils auf Servern ermittelt würden. Und drittens könnten die Diensteanbieter oder Dritt-Anbieter speziell gesicherte Server, sogenannte „Secure Enclaves“, in die Kommunikation zwischenschalten. Diese hätten dann vollen Zugriff auf den Klartext derartig „verschlüsselter“ Inhalte.

In ihrem Gesetzentwurf hat sich die EU-Kommission nicht auf eine genaue Technik festgelegt. Stattdessen könnten die Anbieter beliebige Technologien einsetzen, solange sie die Auflagen erfüllen und unter anderem „wirksam zur Erkennung der Verbreitung von bekannten oder neuen Darstellungen sexuellen Kindesmissbrauchs oder der

Kontaktaufnahme zu Kindern“ beitragen. Alternativ könnten sie kostenlos Techniken nutzen, die ihnen ein noch einzurichtendes EU-Zentrum zur Verfügung stellen würde.

Der Bericht spricht aber klare Empfehlungen aus: Sofort wäre CSS einsetzbar, notfalls könnte ein teilweises Erstellen von Hashes auf Servern stattfinden. Langfristig sollte die EU aber Geld in Forschung stecken, rät das Papier – das in der vorliegenden Fassung noch nicht vollständig finalisiert war. Erfolgsversprechend seien hierbei etwa „Secure Enclaves“ bei den Anbietern oder der Einsatz sogenannter Klassifikatoren („classifiers“). Diese könnten mit Hilfe von Machine Learning selbstständig verdächtige Inhalte aufspüren und an Behörden melden, so die Zukunftsvision.

Klar wird durch das Papier in jedem Fall eines: Von Anfang an stand die Einführung einer anlasslosen Massenüberwachung im Fokus aller Bemühungen.

Über die Autor:in

tomas

Tomas ist in Wien aufgewachsen, hat dort für diverse Provider gearbeitet und daneben Politikwissenschaft studiert. Seine journalistische Ausbildung erhielt er im Heise-Verlag, wo er für die Mac & i, c't und Heise Online schrieb. Er ist unter +49 30 577148268 oder tomas@netzpolitik.org (PGP-Key) erreichbar und twittert mal mehr, mal weniger unter @tomas_np.

Veröffentlicht
16.11.2023 um 12:15

Kategorie
Überwachung

Schlagworte
Chatkontrolle, Client-Side-Scanning, CSS, ende-zu-ende-verschlüsselung, EU Internet Forum, EU-Kommission, Privatsphäre, Verschlüsselung, Ylva Johansson

14 Ergänzungen

Anonymous sagt:
16. November 2023 um 15:35 Uhr

Warum eig. immer sexuelle Darstellungen? Was ist denn mit brutalen Verstümmelungs-, Foltervideos wie Terrororganisationen sie verwenden.

Werden da keine Rechte von Kindern betroffen? Allein daran erkennt man das man mit dem bösen P-Wort eine neue Gruppe geschaffen hat die man als Grund herziehen kann.

Tomas Rudl sagt:
16. November 2023 um 16:40 Uhr

Bislang fehlt etwas mit der Chatkontrolle vergleichbares, in den letzten Jahren hat sich allerdings viel getan und das wird wohl so weitergehen, schätze ich.

(Mutmaßlich) terroristische Inhalte auf Online-Diensten werden bereits per Hash-Datenbank gefiltert: https://netzpolitik.org/2020/terrorismus-im-netz-eine-datenbank-solls-richten/

Passend dazu gibt es eine EU-Verordnung, zum Glück ohne vorgeschriebene automatisierte Mittel: https://netzpolitik.org/2021/terrorpropaganda-eu-gesetz-gegen-terrorinhalte-im-netz-beschlossen/

Tatsächlich ist das EU Internet Forum, in dessen Rahmen das im Artikel besprochene Papier erstellt wurde, einst als Initiative gegen terroristische Inhalte im Netz gegründet worden: https://netzpolitik.org/2016/eu-internet-forum-anbieter-sollen-freiwillig-das-netz-filtern/

Über den geplanten Schwenk von Johansson haben wir damals berichtet: https://netzpolitik.org/2021/kindesmissbrauch-und-terrorismus-mehr-filtern-weniger-verschluesseln/

Und nicht zuletzt fordern manche eine Ausweitung der Chatkontrolle, so sie denn kommen sollte, auf alle möglichen illegalen Inhalte: https://netzpolitik.org/2023/ueberwachung-politiker-fordern-ausweitung-der-chatkontrolle-auf-andere-inhalte/

Okay sagt:
16. November 2023 um 19:51 Uhr

Ich verstehe das Argument nicht. Wo ist bitte der Unterschied zwischen einem Snuff-Film der produziert wird um die sadistischen Bedürfnisse von Menschen zu befriedigen? Ist die Finanzierung und der Konsum solcher Inhalte schlimmer als ein „Posingbild“ wo lt. Polizei selbst einfache Strandfotos drunter fallen können?

Hört sich für mich danach an, als gehe es um die Bestrafung von Perversitäten als um den Schutz von Rechtsgütern. Interessant.

Mr. Tea sagt:
16. November 2023 um 16:49 Uhr

Es steht etwas verklausuliert oben im Artikel: KiPo ist eben IMMER illegal, da muss man nicht diskutieren. Der Abruf von „Terrorinhalten“ kann aber eben auch journalistischen Zwecken oder ähnlichem dienen, und der reine „Konsum“ von (vermeintlichen) „Terrorinhalten“ ist meines Wissens nach gar keine Straftat. Aber wie eben auch im Artikel steht: es wird an allen Fronten daran gearbeitet Verschlüsselung abzuschaffen.

Tomas Rudl sagt:

16. November 2023 um 17:16 Uhr

Genau, u.a. so argumentiert das Papier. Teilweise steht es im Artikel, hier die vollständige Passage:

> The focus on CSA is due to several reasons:
>
> - the material (images and videos) identified as CSA (legally referred to as „child pornography“) is context independent, unlike other types of illegal content such as terrorist material;
> - it is the only illegal content whose mere possession is illegal;
> - industry has been using tools to detect instances of CSA voluntarily for years, as the fight against this type of illegal content has been the least controversial;
> - because of this effort, there is data available to assess the scope of the problem and the impact of foregoing detection measures.

Anonymous sagt:
16. November 2023 um 17:55 Uhr

Welche Definition von „CSA“? Wenn man bedenkt das in vielen EU-Staaten die Definition sich dermaßen stark von einander unterscheidet liest sich das nicht wirklich besser. Dürfen solche Technologien auch bspw. für Strichmännchen eingesetzt werden, obwohl nach EU-Recht nicht zwangsweise illegal sondern Sache der Länder?

Mir gefällt daher das Verschwimmen aller möglichen Inhalte unter einem Begriff nicht. Es ist überhaupt nicht transparent.

Anonymous sagt:
23. November 2023 um 15:12 Uhr

Das wäre tatsächlich interessant zu wissen. Wenn es nach der Position von Deutschland geht dann wäre sowas nicht zu erfassen:

„Der Verordnungsentwurf sollte nur solche Inhalte und Verhaltensweisen erfassen, die EU-weit
verboten sind [...]. Inhalte oder Verhaltensweisen, die nach nationalem Recht nicht
strafbar sind, sind vom Anwendungsbereich des Verordnungsentwurfs auszuschließen.“

Quelle: https://data.consilium.europa.eu/doc/document/ST-8268-2023-INIT/x/pdf

Walter sagt:
17. November 2023 um 10:29 Uhr

Das ist doch Unsinn, sich hier auf „possession“ zu beziehen. Jede chatnachricht ist doch eine „distribution“. Daher trägt das nicht im Chat Kontext.

Live sagt:
17. November 2023 um 22:47 Uhr

„KiPo ist eben IMMER illegal, da muss man nicht diskutieren.“

Wieso muss man da nicht diskutieren? Sie wissen was alles unter „KiPo“ fällt, aber in verschiedenen (EU-)Staaten kein Problem sind, da sie juristisch nicht darunter fallen?

Anonym sagt:
18. November 2023 um 06:45 Uhr

Ich denke da muss man mit Sicherheit darüber diskutieren – wenn abrufen von KiPi IMMER illegal wäre wäre es ja z.B. Strafverfolgung auch illegal denn man könnte ja legal keine Beweise sichern sichten verhandeln. Was Sie so einfahc abtun wäre reiner Täterschutz.

Zum Glück wird darüber diskutiert wenn z.B. wie zur Zeit Richter sich weigern, offensichtlich unschuldige wegen KiPo-Abrufen zu verurteilen.

synapsenkontrolle sagt:
16. November 2023 um 20:54 Uhr

statt Client-Side-Scanning hatte ich erst Client-Side-Scamming gelesen.. o_0

Anonym sagt:
20. November 2023 um 11:17 Uhr

Alles eine Erfindung des Homo Sapiens.
Man brauch ein mobile-phone oder man braucht es nicht.
Wenn man es braucht, reine Linux Handy.

Fento sagt:
23. November 2023 um 18:17 Uhr

KI-Modelle können bald relativ zuverlässig potenziell illegales Material erkennen. Gib einem Textmodell Informationen (Alter, Geschlecht, gefolgte Accounts und Follower) beider Chatpartner zusammen mit dem Chatverlauf in den Kontext (Speech-to-Text

für Skype, Omegle und Co.) und es kann problemlos erkennen, ob hier ein Grooming stattfindet.

Technisch sollte das gar nicht mal schwierig sein, aber es bedeutet, dass alle Interaktionen auf allen zugelassenenen Endgeräten von KI-Modellen ausgewertet werden, um abnormales Verhalten zu erkennen. Alle non-E2E Platformen (Omegle, Roblox, Fortnite Sprachchat) müssen diese KI-Analysatoren serverseitig implementieren, sodass erkannt werden kann, wenn ein Erwachsener mit einem Kind über annormale Sachen spricht. Alle erlaubten Endgeräte müssen KI-Analysatoren clientseitig implementieren, um auch e2e-Kommunikation abzugreifen.

Langfristig wird sowas auf die ein- oder andere Weise kommen, auch China hätte großes Interesse daran. Hier wird unter dem Vorwand von Kinderschutz das größte und umfassendste Vollüberwachungsinstrument der Geschichte eingeführt.
Ist das erstmal Realität, ist es relativ einfach, diese Kontexterkennung auf „Plant jemand einen Terroranschlag“ oder „Denkt jemand schlecht über den Präsidenten“ auszuweiten.

Das Problem ist, dass man mit „Kinderschutz“ ALLES einführen kann und niemand dagegen sein darf. So z.B. die komplett in die Hose gegangene Verschärfung von § 184b, bei der überlastete Gerichte jetzt hauptsächlich Jugendliche und Eltern als Verbrecher behandeln, oder § 184l aka Puppenverbot, welches als sog. Gesinnungsstrafrecht (= Kriminalisierung von Fantasien an leblosen Objekten) den Pädophilen ein Ventil nimmt, mit der Sexualität klarzukommen ohne jemandem zu schaden, und dadurch den Kinderschutz effektiv torpediert.

Das alles ist einer Demokratie nicht mehr würdig und ich mache mir ernsthaft Sorgen, wo das hinführt, wenn die EU diese Pläne weitertreibt.

Hannah sagt:
24. November 2023 um 13:33 Uhr

Secure Enclaves haben eine begrenzte Berechtigung – sie aber auch nur ansatzweise als Alternative zu E2EE darzustellen ist ja wohl ein Skandal...
