Tobias Blicker

Was mir hier fehlt ist die Beleuchtung der Gegenseite. Die EU wird sich der Risiken wohl bewusst sein? Die USA machen es ähnlich? Es könnte sichere Kommunikationskanäle für Sicherheitsbehörden geben? Genügt nicht die Ablehnung der Flächenüberwachung = Anlassbezogen ok? Links zum EU-Vorschlag? Was wiegt schwerer: Terroristen und Kriminelle möglicherweise so zu entdecken oder eine versehentliche Einsichtnahme, die sofort gelöscht werden müsste (wer behält sich sowas)? 2.9 ist das einzige Kapitel was auf diese Bedenken eingeht – es würde wenig bringen wegen einer Verlagerung. Sollte Industriespionage nicht durch interne Systeme unmöglich sein, wer den neuen Bauplan des iPohne xy über Whatsapp versendet, ist halt dann selbst Schuld. Eine Info aus der Gruppe noch: Sicherheitskräfte würden schon jetzt den Datenberg nicht mehr bewältigen können. Würden die Sicherheitsbehörden denn unnütze Daten erhalten? Im Antrag steht, dass die Dienste nur auffällige Daten übermitteln sollen (also selbst kontrollieren sollen).

**Antwort Fachgruppe Digitalpolitik:**

Es wäre einfacher, wenn Kritikpunkte direkt als einzelne, konkrete Fragen/Vorschläge vorgetragen werden würden, idealerweise sogar fortlaufend nummeriert, damit auch später noch auf sie Bezug genommen werden kann.

Ich lese aus deinem Text:

1: Was mir hier fehlt ist die Beleuchtung der Gegenseite. Die EU wird sich der Risiken wohl bewusst sein?

2: Die USA machen es ähnlich?

3: Es könnte sichere Kommunikationskanäle für Sicherheitsbehörden geben?

4: Genügt nicht die Ablehnung der Flächenüberwachung = Anlassbezogen ok?

5: Links zum EU-Vorschlag?

6: Was wiegt schwerer: Terroristen und Kriminelle möglicherweise so zu entdecken oder eine versehentliche Einsichtnahme, die sofort gelöscht werden müsste (wer behält sich sowas)?

7: 2.9 ist das einzige Kapitel was auf diese Bedenken eingeht – es würde wenig bringen wegen einer Verlagerung.

8: Sollte Industriespionage nicht durch interne Systeme unmöglich sein, wer den neuen Bauplan des iPohne xy über Whatsapp versendet, ist halt dann selbst Schuld.

9: Sicherheitskräfte würden schon jetzt den Datenberg nicht mehr bewältigen können. Würden die Sicherheitsbehörden denn unnütze Daten erhalten? Im Antrag steht, dass die Dienste nur auffällige Daten übermitteln sollen (also selbst kontrollieren sollen)

**Ich würde zukünftige Fragesteller bitten, ihre Fragen fortlaufend zu nummerieren, beginnend bei der #10.**

**Zu 1:**1: Was mir hier fehlt ist die Beleuchtung der Gegenseite. Die EU wird sich der Risiken wohl bewusst sein?

„Die EU wird sich der Risiken wohl bewusst sein?“ Das ist ja das Problem, sie sind es sich nicht wirklich bzw wiegeln ab.
~Bastian Große
Technisch nicht sonderlich versierte Entscheidungsträger mit festen ideologisch geprägten Ansichten („*Wir müssen alles mitlesen können, wir müssen alles überwachen, nur so können wir Kriminalität ausmerzen, das Internet ist kein rechtsfreier Raum!*“) fordern hier (mal wieder) Maßnahmen, ohne sich über die wirklichen Folgen im Klaren zu sein. Kritik wird dabei voreilig abgetan, da man sich in meinen Augen gewissermaßen daran gewöhnt hat, dass Datenschützer bei nahezu jedem Vorhaben Schnappatmung bekommen und protestieren. Der Kontrast in der Deutlichkeit der Ablehnung wird leider nicht erkannt.
~Daniel Putz

Tobias Blicker: Die Begründung der EU sollte hier, besser im Antrag, stehen. Die Vorwürfe gegenüber der EU kann man so nicht objektiv prüfen.

**Zu 2:** Die USA machen es ähnlich?
Nein. Verpflichtende Hintertüren für Chats gibt es in diesem Sinne bislang nicht. Zwar wird auf einzelne Unternehmen in den USA Einfluss genommen („*Cisco!! Wir brauchen eine Hintertür in euren Routern, Terroristen überall!!*“, siehe auch Snowden-Leaks, primäre Datenlieferanten der NSA bzw der „Five Eyes“ im Allgemeinen), der Betrieb von Ende-zu-ende verschlüsselten Chats (die außer an den Endgeräten nicht abhörbar sind) ist jedoch nicht untersagt. Man verlässt sich hierbei darauf, Geräte von Verdächtigen im Falle eines Falles zu entsperren und so auf die verschlüsselten Inhalte zugreifen zu können. Ich erinnere an dieser Stelle etwa an einen bekannten Fall aus 2016, als das FBI Apple um Hilfe beim Entsperren eines iPhones bat, Apple sich verweigerte, und am Ende scheinbar doch noch ein anderer Weg gefunden wurde: <https://www.zdnet.com/article/fbi-gets-access-to-seized-iphone-without-apples-help-drops-legal-case/>
Es gilt: Kommunikation ist zunächst einmal sicher verschlüsselt, die Behörden arbeiten aber an Wegen möglichst alle beschlagnahmten Geräte auslesen zu können um dennoch auf die Inhalte zugreifen zu können, indem sie alle Verschlüsselung UMGEHEN statt sie zu brechen. Speziell hierfür gibt es Unternehmen die diverse Lösungen hochpreisig anbieten und von zahlreichen Geheimdiensten frequentiert werden.
~Daniel Putz

Tobias Blicker: Dann könnten kriminelle Staaten, Reiche, das organisierte Verbrechen auch hier Gelder investieren und Systeme knacken. Das gleiche wie also mit Chatkontrolle, nur langsamer und teurer? Laien hingegen, die auch Terroranschläge verüben können, würden durch eine Chatkontrolle ggfs. In die Falle gehen. Unternehmen und Behörden wissen, dass Daten in entsprechenden Systemen nicht sicher sind und können andere nutzen. Wie in Wien hört man ständig, dass ausländische Geheimdienste uns Infos geben, vermutlich vor allem die USA. Dort ist der Datenschutz geringer als hier. Ich las aber auch schonmal, dass unsere Agenten naja sind.

Bastian: selbst für laien wäre es mit ein bisschen recherche trotz chatkontrolle sehr einfach diese regelung zu umgehen. Was ist wenn die Systeme der Chatanbieter nicht in der EU gehosted werden, sondern z.B. In Afrika/China/irgendeinem anderen neutralen Staat? Die EU kann dank funktionsweise des Internets keine Person daran hindern Dienste aus dem Ausland zu nutzen, sie kann es nur erschweren, siehe China. Und wenn bekannt ist das deine Chats überwacht werden und du etwas illegales machen möchtest wirst du doch nicht auf Systeme zugreifen von denen du weißt das sie kompromitiert sind? Und was meinst du das Behörden andere Systeme nutzen sollen? Es sind schließlich alle Systeme betroffen die 1:1 und 1:n Kommunikation erlauben (der kompromissvorschalg schließt einige wie telefon und email aus)

**Zu 3:** Es könnte sichere Kommunikationskanäle für Sicherheitsbehörden geben?Ja die gibt es, als Beispiel haben wir z.b. Den Bundeswehr Messenger genannt, der auf quelloffener Software aufbaut, die Software selbst würde auch unter die Chatkontrolle fallen. Das große Problem an Verschlüsselung ist es das du sie nicht nur für bestimmte Personen ausschalten kannst. D.H das grundlegende Konzept der Software müsste daran angepasst werden das Behörden darauf zugriff bekommen, Da z.B. Fast alle Messenger (Whatsapp, BW Messenger,Signal etc) auf gleichen Konzepten aufbauen, zum Beispiel das der Server/die Firma die die Software betreibt nicht mitlesen kann was in den versandten Nachrichten steht. Behörden Zugriff auf diese Nachrichten zu geben würde bedeuten diese sogenannte ende-zu-ende Verschlüsselung (e2ee) aufzuweichen/aufzubrechen.
~Bastian Große

Tobias Blicker: Es müsste halt ein ganz eigenes System erschaffen werden (ggfs. Durch die EU als Ganzes) und der Gesetzgeber kann selbst bestimmen, was unter die Kontrolle fällt. Dann dauert es halt 5 Jahre. Solange wartet man dann noch.

**Zu 4:** Genügt nicht die Ablehnung der Flächenüberwachung = Anlassbezogen ok?
Selbst bei einer reinen Anlassbezogenen Kontrolle müsste die Verschlüsselung/Kommunikation zu weit aufgeweicht werden das man sie nicht mehr als ende zu ende verschlüsselt betrachten kann. Da macht es kein unterschied ob nur anlassbezogen oder nicht. Hier haben Behörden bessere Methoden anlassbezogene Überwachung zu Unternehmen, siehe Kommentar von Daniel zu 2.
~Bastian Große

Tobias Blicker: Am besten im Antrag aufnehmen.

**Zu 5:**Links zum EU-Vorschlag?Generell geht es in unserem Positionspapier nicht um den EU antrag. Hier sind alle kritiken nochmal von den Piraten zusammengefasst:
- <https://www.patrick-breyer.de/beitraege/chatkontrolle/#aktuelle-entwurf>
- <https://www.patrick-breyer.de/en/lawmakers-across-the-eu-call-on-eu-council-to-reject-the-chat-control-proposal/>
- <https://www.patrick-breyer.de/wp-content/uploads/2024/04/2024-03-28-conseil-csam-compromis-presidence-belge.pdf>
Generell ist da in dem Antrag noch einges weiteres drin was nicht gutzuheißen ist:
Ende des digitalen Briefgeheimnisses.
Als Kommunikationsdienste betroffen sind u.a. Telefonie, E-Mail, Messenger, Chats (auch als Teil von Spielen, auf Datingportalen usw.), Videokonferenzen, Ende-zu-Ende verschlüsselte Messenger sind nicht ausgenommen. Als Hostingdienste betroffen sind u.a. Webhoster, soziale Medien, Video-Streamingdienste, Filehoster und Clouddienste, d.h da fällt dann auch die Parteicloud drunter oder die persönliche icloud die du mit niemandem teilst.

Bei der Chatkontrolle muss nach bekannten Bildern und Videos gesucht werden, verdächtige Nachrichten/Dateien werden der Polizei angezeigt. Die effektictät solcher scanprogramme ist erstaunlich schlecht, 80-90% aller Meldungen sind False Positives (citation needed), und ein Großteil der 10% die Relevant sind, sind Leute die sich gegenseitig Intimfotos teilen.

Tobias Blicker: Beweis?

Die quelle die ich meinte ist leider offline: <https://fedpol.report/de/fedpol-in-zahlen/kampf-gegen-padokriminalitat>

Für 20% CSAM kann ich das hier zeigen: https://www.iccl.ie/news/an-garda-siochana-unlawfully-retains-files-on-innocent-people-who-it-has-already-cleared-of-producing-or-sharing-of-child-sex-abuse-material/

Bei der Chatkontrolle muss auch nach unbekannten Bildern und Videos gesucht werden, verdächtige Nachrichten/Dateien werden der Polizei angezeigt. -> Können viele/alle messenger nicht stemmen, ohne e2ee komplett aufzubrechen. Die Effektivität ist nicht bekannt

Bei der Chatkontrolle muss im Nachrichtentext maschinell nach möglichen Hinweisen auf Kontaktaufnahmen zu Kindern und Jugendlichen gesucht werden, verdächtige Nachrichten werden der Polizei angezeigt. -> Können viele/alle Messenger nicht stemmen, ohne e2ee komplett aufzubrechen. Die Effektivität ist nicht bekannt.

Appstores müssen das Alter ihrer Nutzer überprüfen und Kindern/Jugendlichen unter 16 die Installation von Apps verbieten, die für Anbahnungszwecke missbraucht werden können. -> Das sind im endeffekt Alle Messenger, d.h keine jugendlicher unter 16 darf Whatsapp nutzen. Würde auch zum Ende der Anonymität im Internet führen.

Tobias Blicker: Das wäre ja mal krass, welcher Paragraf meint das?

An sich ist nur von age verification gesprochen im dokument ob jemand ein kind ist oder nicht: <https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF>

Die information mit 16 habe ich von: <https://www.patrick-breyer.de/beitraege/chatkontrolle/#aktuelle-entwurf>

* Bastian

Internet-Zugangsanbieter müssen verpflichtet werden, den Zugang zu verbotenen und nicht zu löschenden Bildern und Videos außerhalb der EU mittels Netzsperren (URL-Sperren) zu blockieren. -> Sind nicht effektiv, jeder 16 Jährige mit 5min google suche kann solche Sperren umgehen (VPN dienst, oder DNS ändern)

Generell wird zusätzlich diese Lösung unglaublich viel Strom(in form von Rechenleistung) verbrauchen für eine Fragliche Wirkung die noch massiv schädigend für die persönliche Freiheit ist im Internet.
~Bastian Große

Der Antrag im Original umfasst (in deutscher Sprache) genau 150 Seiten, bei Interesse:
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0209>
Ich würde ebenfalls auf die Aufarbeitung Anderer, etwa des Abgeordneten Breyer verweisen.
~Daniel Putz

Tobias Blicker: Hier der Direktlink zur Deutschen Version. Sollte auch in den Antrag, um ihn möglichst robust zu machen, am besten soviele fundierte Gegenargumente wie möglich. Ab Seite 25 stehen bspw. 84 Begründungen: https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0008.02/DOC\_1&format=PDF

**Zu 6:** Was wiegt schwerer: Terroristen und Kriminelle möglicherweise so zu entdecken oder eine versehentliche Einsichtnahme, die sofort gelöscht werden müsste (wer behält sich sowas)?Weils ein Verschlüsselungstechnischer Kahlschlag ist, der super einfach auszubauen ist in ein Überwachungstaat ohne einen riesen Benefit zu haben. Solche Maßnahmen werden immer mit Terrorismus/Kinderpornogrpahie/Verbechen begründet, siehe Uploadfilter. -Bastian

**Zu 7:**2.9 ist das einzige Kapitel was auf diese Bedenken eingeht – es würde wenig bringen wegen einer Verlagerung.

**Zu 8:**Sollte Industriespionage nicht durch interne Systeme unmöglich sein, wer den neuen Bauplan des iPohne xy über Whatsapp versendet, ist halt dann selbst Schuld.
Wir reden hier nicht von Whatsapp. Auch zwischen Arbeitskollegen kann es im Unternehmensinternen Chat (Slack, Teams oder was auch immer) theoretisch zum Versenden von entsprechendem Material kommen, auch diese müssten überwacht werden und wäre von der Chatkontrolle nicht ausgenommen.
Selbst wenn Chats zwischen Arbeitskollegen nur Verweise und Referenzen auf schützenswerte Dokumente enthalten sollten, wäre das teils schon kritisch, da es Einblicke in die Funktionsweise der Produkte gibt. Werden hingegen direkt Dokumente und Auszüge aus dem Programmcode übertragen (was absolut keine Seltenheit ist), stellt die mögliche Industriespionage Unternehmen vor ein großes Problem.
Im IT-Bereich wird etwa des öfteren „Pair Programming“ betrieben: Zwei Entwickler teilen den Bildschirm und arbeiten gemeinsam am Programmcode – in diesem Fall genügt die reine Kommunikation (Bildschirminhalt), um nach und nach das komplette Produkt Stückweise zu stehlen. Von Leichtsinn seitens der Mitarbeiter kann dabei nicht geredet werden, da es insbesondere für Remote-Arbeiter der Alltag ist.
~Daniel Putz

**Zu 9:**Sicherheitskräfte würden schon jetzt den Datenberg nicht mehr bewältigen können. Würden die Sicherheitsbehörden denn unnütze Daten erhalten? Im Antrag steht, dass die Dienste nur auffällige Daten übermitteln sollen (also selbst kontrollieren sollen)

Siehe 5. : Die effektivität solcher scanprogramme ist erstaunlich schlecht, 80-90% aller Meldungen sind False Positives, und ein Großteil der 10% die Relevant sind, sind leute die sich gegenseitig Intimfotos teilen.
<https://www.republik.ch/2022/12/08/die-dunklen-schatten-der-chatkontrolle>:
„*Finden die US-Techkonzerne auf diese Weise verdächtiges Material – selbst wenn sie auf freiwilliger Basis danach gesucht haben –, müssen sie es der cyber tipline des National Center for Missing and Exploited Children (NCMEC) melden*“
„*Von knapp 30 Millionen KI-basierten Verdachts­meldungen blieben also nach menschlicher Sichtung 4260 Fälle übrig*“
<https://www.iccl.ie/news/an-garda-siochana-unlawfully-retains-files-on-innocent-people-who-it-has-already-cleared-of-producing-or-sharing-of-child-sex-abuse-material/>
<https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMST17-4176.pdf>
~Bastian Große

Man muss sich auch darüber im Klaren sein: es geht um MILLIARDEN Nachrichten jeden Tag, selbst winzige Fehlermargen sind bei dieser Masse katastrophal. Konkrete Zahlen, weltweit:
- 300milliarden Emails am Tag
- 100milliarden WhatsApp Nachrichten pro Tag
- 7 Milliarden Bilder pro Tag
Auch wenn wir hier „nur“ den Datenverkehr in Europa betrachten müssen, sind die Zahlen erschreckend hoch.
Quellen:
<https://de.statista.com/statistik/daten/studie/868733/umfrage/anzahl-der-taeglich-verschickten-whatsapp-nachrichten-weltweit/>
<https://www.bitkom.org/Presse/Presseinformation/Corona-Jahr-2021-300-Milliarden-Kurznachrichten-in-Deutschland>
Außerdem muss insbesondere bei händischer Prüfung auch gesagt werden: Lieber wird von Unternehmen zu viel als zu wenig gemeldet, denn wenn illegale Inhalte nicht gelöscht/gemeldet werden, drohen erfahrungsgemäß empfindliche Strafen, wohingegen hohe Quoten unnötiger Meldungen nicht geahndet werden.
~Daniel

Tobias Blicker: Generell würde ich den Antrag mit mehr Informationen, wie bspw. aus 9., robuster gegen Gegenmeinungen machen. Die Fachgruppe kann diesen bis zum Debattenende jederzeit mit 2/3-Mehrheit abändern (dann mir mitteilen).