erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Kirsten Bock, Christian Ricardo Kühne, Rainer Mühlhoff, Měto Ost, Jörg Pohle, Rainer Rehak

Kritik an offizieller Datenschutz-Folgenabschätzung für die Corona-Warn-App

Es gibt sie nun, die lang erwartete App zur Kontaktverfolgung. Was ihr fehlt, ist eine hinreichende Datenschutz-Folgenabschätzung. Dazu müssen nicht nur die App selbst, sondern auch dazugehörige Serversysteme, Anwendungen und Infrastrukturen betrachtet werden. Der Gastbeitrag erklärt, warum und wie das idealerweise geschehen kann. Quelloffenheit der Technik allein reicht längst nicht.

Am 16. Juni war es endlich soweit, in ganz Deutschland und auch darüber hinaus blickte man auf die nun veröffentlichte Corona-Warn-App. Nach wochenlanger Diskussion um Nutzen, Technik und Architektur konnte sie endlich installiert und genutzt werden, was Stand 29. Juni 2020 bereits über vierzehn Millionen Mal getan wurde. Die halbe Welt berichtete über den deutschen Erfolg bei der digital-automatisierten Kontaktverfolgung.

Kennzahlen zur Corora-Warn-App
Stand 04. August 2020, Quelle: Robert Koch Institut

191.025
Anrufe bei der technischen Hotline und der Verifizierungshotline im Zeitraum 16. Juni bis 03. August 2020.

1.128
tägliche Anrufe (im Durchschnitt)
im Zeitraum 27. Juli bis 03. August 2020.

1.052
ausgegebene TeleTANs zur Verifizierung eines positiven Testergebnisses seit dem 16. Juni 2020.

16.600.000
aktuelle Downloads der Corona-App

Aber wie so oft ist nicht alles Gold, was glänzt, und nicht jeder kennt den Unterschied zwischen Datenschutz und IT-Sicherheit. Das FIfF hat daher eine Analyse samt konstruktiver Anmerkungen und Vorschläge[1] zur offiziellen Datenschutz-Folgenabschätzung (DSFA) für die im internationalen Vergleich sehr populäre Corona-Warn-App[2] veröffentlicht. Darin spart das FIfF nicht mit grundsätzlicher und konkreter Datenschutz-Kritik, verteilt aber auch Lob für den gesamten Entwicklungsprozess.

Der Beitrag erklärt den Sinn und Zweck einer DSFA und erläutert auch, welche nach wie vor gültigen Ergebnisse eine eigene DSFA, die das FIfF bereits im April veröffentlichte, erbracht hat. Eine DSFA ist dabei keine Fingerübung im akademischen Diskurs, sondern eine notwendige und gesetzliche Anforderung an Datenprojekte, die Informationen von Menschen verarbeiten – denn Datenschutz ist Grundrechtsschutz.

Eine ausführlichere Auseinandersetzung mit der DSFA folgt in Form eines Interviews mit Kirsten Bock (ab Seite 13).

Datenschutzfragen dezentraler Corona-Tracing-Apps

„Es geht nicht um Privatsphäre, sondern es geht darum, eine Technik sozial beherrschbar zu machen."
Wilhelm Steinmüller (1934–2013)[3]

Gesellschaftliche Implikationen durch Datenschutz-Folgenabschätzungen diskutierbar machen

Mehrere Wochen kreiste die Diskussion über die Eindämmung der Corona-Pandemie um den Einsatz technischer Hilfsmittel, insbesondere von sogenannten Corona-Tracing-Apps. Diese sollen automatisiert die epidemiologisch relevanten Kontaktereignisse von NutzerInnen aufzeichnen und es so erlauben, im Infektionsfall zeitnah und rückwirkend die exponierten Kontaktpersonen zu warnen und zu isolieren. Bislang wird das sogenannte Contact-Tracing manuell von MitarbeiterInnen der Gesundheitsbehörden vollzogen, also etwa anhand der Erinnerung der Infizierten und anschließender Warnung per Telefon. In einigen Ländern, zum Beispiel China, werden auch weitere Informationsquellen genutzt wie beispielsweise Kreditkartendaten oder Reiseinformationen. Diese mühsame Arbeit kann, so die Vision, durch den Einsatz von Apps wesentlich beschleunigt werden.

Auch wenn die konkrete Tauglichkeit einer solchen App für diesen Zweck sowohl epidemiologisch als auch technisch noch umstritten ist und die Gefahr einer grundsätzlichen gesellschaftlichen Gewöhnung an Contact-Tracing besteht, soll es an dieser Stelle nicht um ein generelles *Ob*, sondern ein *Wie* einer solchen App gehen. Denn erst bei der Betrachtung der konkreten technischen Umsetzung lassen sich individuelle und gesellschaftliche Konsequenzen[4] analysieren. Die Erkenntnisse können dann wiederum in Form von Anforderungen zurück in die konkrete Ausgestaltung des Verfahrens fließen.

Datenschutz und seine Verankerung in der Gesetzgebung ist ein Garant der Grundrechte und Grundfreiheiten im digitalen Zeitalter. Er bezieht sich nicht nur auf individuelle, sondern auch auf kollektive Rechte. Datenschutz hält die funktionale Differenzierung[5] moderner Gesellschaften aufrecht, indem er strukturelle Machtasymmetrien problematisiert und somit gesellschaftliche Grundfunktionen absichert.

Im Unterschied zu Fragen der IT-Sicherheit geht es dem Datenschutz weniger um externe Angriffe auf Systeme und Daten, sondern um Grundrechtseinschränkungen durch die Datenverarbeitung selbst. Im Fokus steht deshalb nicht primär die „Privatheit" des einzelnen Datensubjekts, sondern die gesamtgesellschaftlichen, strukturellen Auswirkungen und Machteffekte einer Datenverarbeitung. Eine Datenschutzanalyse geht somit prinzipiell von der verarbeitenden Organisation als der primären Risikoquelle aus, um den Blick von dort schließlich auch auf Plattformen, DienstleisterInnen, NutzerInnen und externe Dritte zu richten.

Datenschutz-Folgenabschätzung

Auch wenn die technischen Eigenschaften der Tracing-Apps, darunter sogar ihre genaue Zweckbestimmung, noch nicht abschließend ausgehandelt sind, müssen die datenschutz- und somit grundrechtsrelevanten Folgen dieses Vorhabens nach wie vor detailliert diskutiert werden. Für diese Art der Analyse gibt es in der DSGVO das Instrument der Datenschutz-Folgenabschätzung. Dort heißt es in Artikel 35 DSGVO:

> *(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.*[6]

Für das methodische Vorgehen im Rahmen einer DSFA gibt es unterschiedliche Ansätze. In Deutschland wird dafür von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder das von ihr ausgearbeitete *Standard-Datenschutzmodell* (SDM)[7] empfohlen, an dem auch wir uns im Folgenden orientieren. Dieses verlangt zunächst eine Schwellwertanalyse, um zu klären, inwiefern eine DSFA für ein gegebenes Datenverarbeitungssystem nicht nur gesellschaftlich wünschenswert, sondern auch datenschutzrechtlich gefordert ist. Weil mit den Contact-Tracing-Apps sowohl eine neuartige Technologie als auch personenbezogene Daten in großem Umfang und im Infektionsfall sogar medizinische Daten verarbeitet werden, ist dies hier unzweifelhaft der Fall.

Trotzdem hatte noch bis Ende April keine verantwortliche Stelle eine DSFA für eine der in Deutschland diskutierten Apps vorgelegt. Um die gebotene Aufmerksamkeit auf dieses Thema zu legen, haben wir im April kurzerhand eine Muster-DSFA zur Corona-App[8] erarbeitet und in die öffentliche Diskussion eingebracht.

Im ersten Schritt wird der Zweck des gesamten Datenverarbeitungsverfahrens definiert, in diesem Falle ausschließlich das Erkennen und Unterbrechen von Infektionsketten. Danach gilt es den Kontext der Verarbeitung herauszuarbeiten. Dies umfasst nicht nur die allgemeine gesellschaftliche und politische Lage sowie technische Umstände, sondern auch explizit die verschiedenen Akteure und ihre Interessen. Erst auf dieser Grundlage kann später eine fundierte Analyse von Risiken und Angriffsszenarien erstellt werden.

Sodann müssen Annahmen und Anwendungsfälle für die Verarbeitung erarbeitet werden, um daran anschließend die Verarbeitungstätigkeit im Detail zu beschreiben. Dabei ist zu beachten, dass Verfahren in Teilschritte zu zerlegen sind, von denen nicht alle technikgestützt ablaufen müssen. Im vorliegenden Falle umfasst das Verfahren nicht nur die App, sondern auch die dazugehörigen Serversysteme, Fachanwendungen und Infrastrukturbestandteile wie etwa Betriebssysteme oder technische Kommunikationsbeziehungen. Auf dieser Basis werden dann Rechtsgrundlagen und die Verantwortlichkeit der Verarbeitungstätigkeit diskutiert sowie rechtliche Anforderungen erarbeitet.

All diese Vorarbeiten kombinierend werden Schwachstellen, Gefahren und Risiken der Verarbeitung entwickelt. Damit sind Risiken bezüglich der Grundrechte der Betroffenen gemeint, und zwar aller Grundrechte. Auf die Risikoanalyse aufbauend werden dann Schutzmaßnahmen für die Rechte der Betroffenen bestimmt und zuletzt Empfehlungen für die Verantwortlichen aufgeführt. Die Empfehlungen umfassen insbesondere die besonders problematischen Aspekte, etwa Risiken, für die keine Schutzmaßnahmen existieren.

Zentral oder dezentral?

Aus Gründen der Minimierung des Grundrechtseingriffs und zur Vereinfachung der Analyse gehen wir in unserer DSFA von einem eng umrissenen Zweck für die Datenverarbeitung aus: die Warnung von Personen, die mit Infizierten Kontakt hatten. Die Grundfunktionalität einer solchen App wird im Idealfall umgesetzt, indem das Smartphone in regelmäßigen Abständen über den *Bluetooth-Low-Energy-Beacons*-Standard wechselnde Zeichenfolgen (temporäre Kennungen, tempIDs) via Bluetooth versendet und entsprechend die temporären Kennungen (tempIDs) von anderen Apps empfängt, sofern diese örtlich nah genug sind. Diese Daten ermöglichen eine Kontaktnachverfolgung; aus Dauer und Nähe des Kontakts soll ein Ansteckungsrisiko berechnet werden. Ortsinformationen, also zum Beispiel der GPS-Standort, werden durch dieses System nicht erhoben.

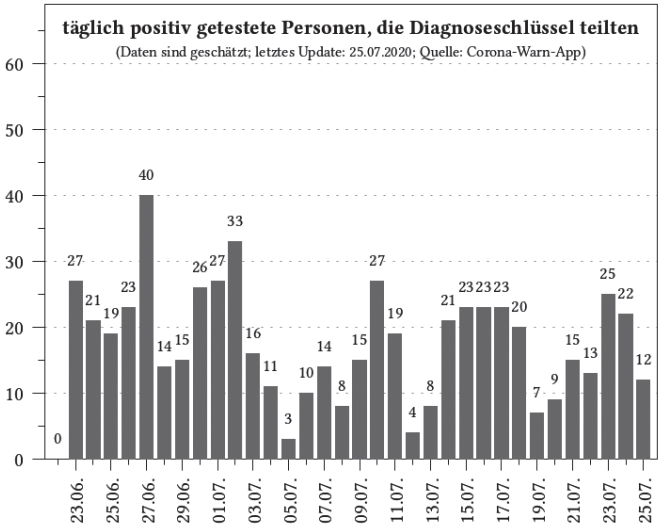
An dieses grundlegende Prinzip zur Detektion von Kontaktereignissen mittels Bluetooth schließen sich nun technische Fragen an, in denen verschiedene Varianten diskutiert wurden. Im Mittelpunkt der Diskussion stand die Frage, ob die Berechnungen des individuellen Expositionsrisikos lokal auf den Mobiltelefonen der NutzerInnen oder serverseitig stattfindet. Damit hängt auch die Frage zusammen, wie genau die exponierten NutzerInnen kontaktiert werden, um sie zu warnen.

In der zentralen Architektur werden im Fall der positiven Testung alle Kontaktereignisse von der App der infizierten Person auf einen Server hochgeladen. Dieser Server berechnet das Expositionsrisiko für alle Kontakte dieser Person und informiert diese dann aktiv. Der Server hat in dieser Variante somit Kenntnis der Infizierten, derer Kontakte und des sozialen Graphen.

Die dezentrale Architektur dagegen sieht vor, dass im Falle der positiven Testung nur die von der Person in den vergangenen vierzehn Tagen ausgesendeten temporären Kennungen (tempIDs) auf den Server geladen werden. Die anderen Apps laden

sich regelmäßig einen Datensatz aller tempIDs von infizierten NutzerInnen herunter und berechnen lokal auf ihrem Smartphone, ob ein Risiko der Ansteckung vorliegt. Der Server kennt in dieser Variante nur die temporären Kennungen der Infizierten, er kann weder ihre Kontakthistorie noch das Kontaktnetzwerk der NutzerInnen nachvollziehen. Aus diesem Grunde ist die dezentrale Variante deutlich datenschutzfreundlicher.

Unsere DSFA betrachtet nur den dezentralen, grundrechtsschonenderen Ansatz, der inzwischen von Ländern wie etwa Österreich, Schweiz, Estland und seit Ende April auch von Deutschland verfolgt wird.



Quelle: https://micb25.github.io/dka/, CC BY-NC-SA

Zentrale Erkenntnisse

Im Folgenden sollen vier wichtige Ergebnisse unserer DSFA vorgestellt werden.

1. Die häufig beteuerte Freiwilligkeit der App-Nutzung ist ein voraussetzungsreiches Konstrukt, das sich in der Praxis als Illusion herausstellen kann. So ist vorstellbar und wird auch bereits diskutiert, dass die Nutzung der App als Bedingung für die individuelle Lockerung der Ausgangsbeschränkungen gelten könnte. Das Vorzeigen der App könnte als Zugangsbedingung für öffentliche oder private Gebäude, Räume oder Veranstaltungen dienen. Eine solche Verwendungsweise wäre mitunter nicht durch den Zweck des Systems gedeckt, könnte aber durch dritte Akteure (z. B. Arbeitgeber oder private Veranstalter) in Kraft gesetzt werden. Dieses Szenario würde eine implizite Nötigung zur Nutzung der App bedeuten und zu einer erheblichen Ungleichbehandlung der Nicht-NutzerInnen führen; die ohnehin vorhandene „digitale Schere" zwischen Smartphone-BesitzerInnen und -Nicht-BesitzerInnen würde sich hiermit auf weitere Lebensbereiche ausweiten. Zudem könnte der Zweck des Systems unterminiert werden, wenn NutzerInnen aus Angst vor Nachteilen ihr Smartphone absichtlich nicht bei sich führten oder abwechselnd verschiedene Geräte nutzten. Nur durch eine flankierende Gesetzgebung, die diese und andere Zweckentfremdungen effektiv unterbindet, ist dieses Risiko abzumildern.

   Hierbei ist darauf hinzuweisen, dass die informierte Einwilligung kein geeigneter rechtlicher Rahmen für eine freiwillige App-Nutzung ist. Denn die informierte Einwilligung externalisiert das Risiko der (Grundrechts-)Folgen sowie die Abwägung zwischen Nutzen und Folgen auf die Betroffenen. Dabei käme es darauf an, gerade diese Abwägung zum Gegenstand demokratischer Aushandlung zu machen. Als Rechtsgrundlage wäre deshalb ein Gesetz erforderlich, in dem die (demokratisch legitimierte und kontrollierte) GesetzgeberIn die Verarbeitung festlegt und auch deren Grenzen definiert.

2. Ohne Intervenierbarkeit (Einschreitbarkeit) und enge Zweckbindung ist der Grundrechtsschutz gefährdet: Es besteht ein hohes Risiko fälschlich registrierter Expositionsereignisse (falsch Positive durch Wände, Masken oder Laborfehler), die zu Unrecht auferlegte Selbst-Quarantäne zur Folge hätten. Um dem zu begegnen, bedarf es rechtlicher und faktischer Möglichkeiten zur effektiven Einflussnahme, etwa das Zurückrufen falscher Infektionsmeldungen, die Löschung falsch registrierter Kontaktereignisse oder das Anfechten möglicher anderer Konsequenzen.

3. Alle bislang besprochenen Varianten einer Corona-App unterliegen der DSGVO, denn sie verarbeiten personenbezogene Daten. Alle Daten auf einem Smartphone sind personenbezogen, nämlich bezogen auf die NutzerIn des Gerätes. Die gilt unabhängig davon, ob Beteiligte die versendeten Zeichenfolgen auf eine Person zurückführen können oder ob das Gerät gut vor dem Zugriff Dritter abgesichert ist. Und weil nur diejenigen Personen Daten an den Server übertragen, die als infiziert diagnostiziert wurden, handelt es sich bei diesen hochgeladenen Daten sogar um Gesundheitsdaten.

   Nur durch ein Zusammenspiel organisatorischer, rechtlicher und technischer Maßnahmen kann der Personenbezug wirksam und irreversibel von den hochgeladenen Daten abgetrennt werden, so dass sie letztlich auf dem Server nur noch als „infektions-indizierende Daten ohne Personenbezug" ankommen. Dieses Anonymisierungsverfahren kann diverse Formen annehmen, muss jedoch kontinuierlich datenschutzrechtlich durch die zuständigen Aufsichtsbehörden prüfbar sein: Organisatorisch müssen die Verantwortlichen in strategischer und die BetreiberIn(nen) in operativer Hinsicht eine Mischstruktur etablieren. Die Verantwortliche – etwa das RKI – könnte strategisch beispielsweise zwei unterschiedliche BetreiberInnen auswählen: Eine betreibt die Eingangsknoten im Netzwerk und trennt die Metadaten ab, darunter die IP-Adressen, die andere betreibt den eigentlichen Server. Auf der Ebene der BetreiberInnen muss dann operativ auf eine angemessene Abteilungsstruktur und Funktionstrennung geachtet werden, die die informationelle Gewaltenteilung innerhalb der Organisation – also die funktionale Differenzierung[9] – durchsetzen. Rechtlich müssen die BetreiberInnen unabhängig sein, keine eigenen Interessen an den Daten haben und vor Pflichten zur Herausgabe von Daten geschützt sein, auch gegenüber staatlichen Sicherheitsorganen. Technisch muss die BetreiberIn die Trennung so umsetzen, dass die Uploads nicht protokolliert werden können, weder auf dem Server noch in ihrem Netzwerk. All diese Maßnahmen müssen durch ein Datenschutzmanagementsystem kontinuierlich prüfbar gemacht und auch geprüft werden.

4. Die Rolle der Plattformanbieter Apple (iOS) und Google (Android) ist kritisch zu diskutieren und über den gesamten Verarbeitungsprozess hinweg zu begleiten. Eine Bluetooth-basierte Corona-Tracing-App ist aus technischen Gründen auf die Kooperation der Plattformanbieter angewiesen, da der Zugriff auf das Bluetooth-Modul der Geräte auf Betriebssystemebene ermöglicht werden muss. Diese Machtposition haben die Plattformanbieter in den vergangenen Wochen genutzt, um gegen zahlreiche Regierungen eine dezentrale und somit datenschutzfreundlichere Architektur zu erzwingen. Damit ist das Datenschutzrisiko, das von den Plattformbetreibern selbst ausgeht, in der öffentlichen Diskussion weitestgehend aus dem Blick geraten. Als Betriebssystemhersteller ist es prinzipiell möglich (und auch realistisch, wie die DSFA zeigt), dass Google und Apple an die Kontaktinformationen gelangen und daraus Informationen über Infektionsfälle und Expositionsrisiken ableiten können. Eine kritische Begleitung der Rolle von Apple und Google erfordert daher eine umfassende Sensibilisierung für dieses Problem und die rechtliche Verpflichtung der Unternehmen, sich datenschutzkonform zu verhalten.

Diskussion in gesellschaftlicher Breite

Insbesondere die quelloffene Entwicklung von Server und Apps nebst allen ihren Komponenten – beispielsweise als freie Software – ist eine wesentliche Voraussetzung dafür, dass nicht nur für Datenschutzaufsichtsbehörden die nötige Transparenz bezüglich der Umsetzung der Datenschutz-Grundsätze vorliegt, sondern auch für die Betroffenen und die Öffentlichkeit insgesamt. Diese Datenschutz-Folgenabschätzung zeigt aber auch, dass eine Fokussierung allein auf die Quelloffenheit der Technik die durchaus größeren gesellschaftlichen Implikationen des gesamten Verfahrens verschleiern kann. Nur Datenschutz-Folgenabschätzungen können Derartiges offenlegen und sollten in diesem, aber auch in anderen ähnlich folgenreichen Datenverarbeitungsprojekten veröffentlicht werden, damit sie nicht nur von den Datenschutz-Aufsichtsbehörden, sondern auch in gesellschaftlicher Breite und sozialwissenschaftlicher Tiefe diskutiert werden können.

Anmerkungen

1 *https://www.fiff.de/presse/dsfa-corona-cwa*
2 *https://github.com/corona-warn-app/cwa-documentation/blob/master/translations/scoping_document.de.md*
3 *https://www.datenschutzzentrum.de/interviews/steinmueller/index.html*
4 *https://www.fiff.de/presse/dsfa-corona*
5 *https://de.wikipedia.org/wiki/Funktionale_Differenzierung*
6 *https://dejure.org/gesetze/DSGVO/35.html*
7 *https://www.datenschutzzentrum.de/sdm/*
8 *https://www.fiff.de/presse/dsfa-corona*
9 *https://de.wikipedia.org/wiki/Funktionale_Differenzierung*

Quelle: https://netzpolitik.org/2020/contact-tracing-apps-kritik-an-datenschutzfolgenabschaetzung-fuer-die-corona-warn-app/

Ingo Dachwitz interviewt Kirsten Bock

„Risiken und Maßnahmen nicht ausreichend dargelegt“

Vieles ist gut gelaufen bei der Entwicklung der Corona-Warn-App, doch aus Sicht des Datenschutzes gibt es noch Luft nach oben, findet Kirsten Bock. Im Interview kritisiert sie die Datenschutz-Folgenabschätzung (DSFA) der Anwendung und fordert eine gesetzliche Grundlage, um möglichen Missbrauch zu verhindern.

Noch nicht ausgereift

netzpolitik.org: *Mit dem Start der Corona-Warn-App Mitte Juni wurde auch die Datenschutz-Folgenabschätzung veröffentlicht. Telekom, SAP und Robert-Koch-Institut sind damit einer Forderung der Zivilgesellschaft[1] gefolgt. Was ist Ihr erster Eindruck von dem mehr als hundertseitigen Dokument?*

Kirsten Bock: Erstmal freuen wir uns, dass die DSFA der Corona-Warn-App[2] veröffentlicht wurde. Das ist eine wichtige Entscheidung. Was man aber vorweg schon sagen kann, ist, dass sich das Team offensichtlich zum ersten Mal mit einer Datenschutz-Folgenabschätzung befasst hat und – um es mal positiv zu formulieren – versucht hat, sich dem Ziel zu nähern. Aus meiner Sicht ist das jedoch noch keine ausgereifte DSFA.

netzpolitik.org: *Wo liegt das Problem?*

Kirsten Bock: Dem Anspruch nach ist dies eine verpflichtende DSFA nach Artikel 35 der Datenschutzgrundverordnung. Damit gehen bestimmte methodische Vorgaben einher. Der Artikel schreibt zum Beispiel vor, dass die Prüfung vor dem Start einer Technologie durchzuführen ist und enthält insofern auch eine Vorgabe, wie man Privacy by Design materiell umsetzt. Das ist in diesem Fall ganz offensichtlich nicht passiert.

Die Datenschutz-Folgenabschätzung ist – so wie ich das lese – nachträglich erstellt worden. Das ist eigentlich nicht Sinn und Zweck der Sache. Die Verantwortlichen sehen ein „lebendes Dokument“ und wollen die Folgenabschätzung fortführen. Das ist positiv, aber ein Minimum des Notwendigen für neue, eigenständige Komponenten. Eine DSFA ist eigentlich mit einem klaren Ergebnis abzuschließen und wird danach Gegenstand des Datenschutz-Managementsystems der Verantwortlichen.

netzpolitik.org: *Nun war der Zeitraum für die Entwicklung der Tracing-App aber auch ein sehr kurzer.*

Kirsten Bock: Das stimmt natürlich. Aber es war von Anfang an klar, dass man eine hohe Zahl von Nutzern dafür gewinnen will.