Zeitschrift: Schweizer Monat : die Autorenzeitschrift für Politik, Wirtschaft und Kultur

Band: 103 (2023)

Heft: 1109

Artikel: "Künstliche Intelligenz wird meist zur Überwachung eingesetzt"

Autor: Grob, Ronnie

DOI: https://doi.org/10.5169/seals-1050562

«Künstliche Intelligenz wird meist zur **Überwachung** eingesetzt»

Die Präsidentin der Messaging-App Signal, Meredith Whittaker, warnt vor der Anwendung von KI. Sie will grossen Unternehmen, die mit Regierungen verbunden sind, keinen Freibrief ausstellen.

Interview von Ronnie Grob

Die Messaging-App Signal bietet Kunden Informationssicherheit. Nicht einmal Signal kann nach eigenen Angaben herausfinden, was zwei Personen sich in der App sagen oder schreiben. Gibt es Regierungen, die Sie drängen, ihnen Informationen über Ihre Kunden zu geben, und Sie bitten, Hintertüren einzubauen?

Wie jedes andere Technologieunternehmen erhalten auch wir häufig Anfragen von Regierungen nach Informationen. Der beste Weg, die Privatsphäre der Kommunikation im digitalen Raum sinnvoll zu schützen, besteht darin, sicherzustellen, dass wir diese Informationen nicht haben. Wir verschlüsseln nicht nur den Inhalt der Nachrichten, also das, was Sie sagen, sondern auch die Informationen darüber, wer Sie sind, also die Metadaten: Ihren Namen, Ihre Profilinformationen, Ihre Kontaktliste und die Mitglieder Ihrer Gruppenchats. Wir sind nicht in der Lage, diese Informationen zur Verfügung zu stellen, da wir sie nicht besitzen. Wenn die Regierung mir eine Waffe an den Kopf hält, müsste sie schiessen. So funktioniert die Ende-zu-Ende-Verschlüsselung.

Signal wird häufig von autoritären Regierungen blockiert. Welche Länder blockieren es derzeit?

Im Moment ist es zumindest in China und im Iran blockiert, aber ich habe gerade keine aktuelle Liste aller Länder. Wo immer die Zentralmacht befürchtet, dass abweichende Meinungen oder ehrliche Äusserungen eine Bedrohung für sie darstellen, wird versucht, gegen Abweichler vorzugehen. Andersdenkende brauchen natürlich Redefreiheit und freie Meinungsäusserung. Und Räume, in denen Menschen ehrlich miteinander diskutieren können. In ihrem Versuch, abweichende Meinungen und Äusserungen, die sie als bedrohlich empfinden, zu unterdrücken, greifen sie die Instrumente an, die deren Verbreitung ermöglichen.

In China geht der Trend dahin, alle Aktionen auf dem Smartphone zu erledigen, indem man die eine Super-App, WeChat, nie verlässt. Sehen Sie diesen Trend auch im Westen aufkommen, so wie Elon Musk versucht, Twitter zu einer Super-App namens X zu entwickeln?

Leute reden seit Jahren darüber, und wir haben immer noch keine Super-App. Es gibt Vorbilder wie WeChat – das natürlich sehr eng mit Peking verbunden ist – und in Japan gibt es Line, in Südkorea Kakao. Das sind Apps, die zu einer bestimmten Zeit entstanden sind, als es noch nicht viel Wettbewerb auf dem Markt gab, und die in staatliche Dienstleistungen integriert sind. Sie sind nicht in dem besonderen Kontext entstanden, in dem sich die in den USA vorherrschende Technologiebranche entwickelt hat. Ich

glaube nicht, dass es viel Hoffnung auf eine Super-App gibt, die plötzlich auftaucht, die Konkurrenz verdrängt und dann mehrere Märkte in den USA dominiert.

Warum sollte ich Signal und nicht WhatsApp oder Telegram verwenden?

Telegram macht eine Menge Aufhebens um seine Datenschutzversprechen, aber letztendlich ist es keine sichere App – fast alles auf Telegram wird im Klartext gesendet, was bedeutet, dass es, wenn es dazu gezwungen wird, Daten mit Regierungen teilen wird. Daher kann es leicht zu Verletzungen der Privatsphäre kommen. WhatsApp verwendet das Signalprotokoll zur Verschlüsselung von Nachrichteninhalten, nicht aber zur Verschlüsselung von Metadaten. Und wie wir wissen, sind Metadaten ausserordentlich aufschlussreich. Und seien wir ehrlich, es gehört zu Meta. Es ist also nicht undenkbar, dass es die Metadaten und andere Informationen, über die es verfügt, mit den ausserordentlich invasiven Überwachungsdaten kombinieren könnte, die von anderen Meta-Eigentümern wie Facebook oder Instagram gesammelt werden. Der grosse Unterschied ist, dass wir ein gemeinnütziges Unternehmen sind, das sich bemüht, überhaupt keine Daten zu haben.

Verwendet Signal künstliche Intelligenz (KI)?

Signal verwendet ein kleines maschinelles Lernmodell, das eigentlich Teil unserer Werkzeuge für die Medienbearbeitung ist. Es ermöglicht den Nutzern, auf eine Schaltfläche zu klicken, um Gesichter auf einem Foto automatisch unkenntlich zu machen; es wird lokal auf Ihrem Telefon ausgeführt. Wenn Sie z.B. ein Foto von einer Party machen, auf der Sie nicht jeden kennen, und Sie keine Zustimmung zur Weitergabe biometrischer Gesichtsdaten haben, können Sie auf eine Schaltfläche klicken, und das Modell hilft Ihnen, Gesichter zu erkennen und unkenntlich zu machen, so dass Sie Ihre Privatsphäre wahren können. Das ist eine schöne und nützliche Anwendung von KI, die keine Daten an ein App-Unternehmen sendet.

Was ist also das Problem mit der KI?

Wenn KI-Systeme eingesetzt werden, dienen sie in der Regel der Überwachung. Sie erstellen Profile der Gesichter von Menschen und erstellen Daten darüber, wessen Gesicht das ist oder auf welche Art von Person dieses Gesicht hinweist. Sie werden für Bewertungen oder für andere Zwecke verwendet, die an sich schon Überwachung sind. Um diese KI-Systeme zu entwickeln, muss man zunächst über grosse Datenmengen verfügen, um diese Systeme zu trainieren und zu informieren, damit sie kalibriert werden können. Die Metastasierung der KI als eine Art dominante und sehr gehypte Form der Technologie steht im Widerspruch zur Gewährleistung eines echten Datenschutzes. Sie festigt und erweitert das Geschäftsmodell der Überwachung, denn die unersättliche Nachfrage nach Daten führt natürlich zu mehr Überwachung, mehr Sammlung und Erzeugung von Daten.

Welche Probleme hat die KI ausser der Überwachung noch?

Die Dinge, die wir heute als KI bezeichnen, sind Unternehmenstechnologien, die sich auf ausserordentlich konzentrierte Ressourcen stützen, zu denen nur eine Handvoll Unternehmen, hauptsächlich in den USA und China, Zugang haben. Sie stützen sich auf leistungsstarke Rechensysteme und riesige Datenmengen, die nicht einfach aus dem Regal genommen oder aus einer Datenbank gekratzt werden, sondern akribisch und mühsam organisiert und beschriftet werden. Diese Daten werden dann von einer grossen Zahl menschlicher Arbeitskräfte ausgewertet, was wiederum sehr teuer ist. Daher ist die Einstiegshürde für KI in grossem Massstab sehr hoch, und nur eine Handvoll Unternehmen kann sie überwinden. Aus diesem Grund ist Open AI, das als gemeinnützige Organisation begann, heute Teil von Microsoft, und Anthropic gehört zu Google. Deshalb sind nur wenige Unternehmen, die über diese Ressourcen verfügen, in der Lage, diese Modelle von Grund auf zu entwickeln.

Warum ist das gefährlich?

Weil wir die Schlüssel für unglaublich wichtige gesellschaftliche Entscheidungen und Weichenstellungen an eine Handvoll Überwachungsunternehmen weitergegeben haben, die letztlich von Profit und Wachstum und nicht vom sozialen Nutzen getrieben werden. Und wir wissen, dass diese Systeme eingesetzt werden, um diese Ziele zu erreichen, selbst wenn sie wichtige gesellschaftliche Werte untergraben. Diese Hauptgefahr könnte von KI-Systemen ausgehen, die zunehmend Arbeitnehmer überwachen und bestrafen und ihnen Löhne abpressen. Der Einsatz von generativen KI-Systemen wird kreative Berufe wie Journalismus, Kunst, Schriftstellerei usw. unterminieren. In der Polizeiarbeit und in militärischen Konflikten wird KI eingesetzt, um Proteste und abweichende Meinungen zu unterdrücken, um die Ziele der sozialen Kontrolle zu fördern. Wir könnten eine ganze Litanei von Systemen aufzählen, die so kalibriert sind, dass sie den Interessen der Mächtigen auf Kosten derjenigen dienen, die weniger Macht haben. Wir sollten sehr vorsichtig sein, wenn es um die Art von sofortigem Vertrauen geht, das wir in die Hände dieser Unternehmen legen.

Big Tech und Regierungen fordern eine Regulierung der KI. Aber geht es dabei nicht auch darum, mögliche Konkurrenz durch Open-Source-KI-Projekte zu unterdrücken?

Es gibt keine klare Definition dafür, was Open-Source-KI-

«Ich sehe, zumindest in den USA, dass wir die Überwachungsunternehmen und die Überwachungsindustrie nicht ernsthaft von der Regierung trennen können.»

Meredith Whittaker

Meredith Whittaker, fotografiert von Florian Hetz.

Projekte bedeuten. Meta hat zum Beispiel sein Large Language Model LLaMA veröffentlicht und als Open Source bezeichnet, obwohl nur sehr wenige Informationen über das Modell veröffentlicht wurden. Open-Source-KI ermöglicht es nicht jedem, über die notwendigen Ressourcen zu verfügen, um KI von Grund auf zu entwickeln. Die unglaublich wichtigen Entscheidungen über Modellgewichte, über Daten und darüber, wie diese Modelle kalibriert und trainiert werden, liegen derzeit in den Händen der grossen Unternehmen und sind niemals Open Source.

Wie wichtig ist Open Source für Signal?

Open Source bietet zwei Dinge, die im allgemeinen gut sind: Es ermöglicht Transparenz, so dass Sie den Code und möglicherweise andere Dokumentationen und Ressourcen überprüfen können, was für die Rechenschaftspflicht sehr hilfreich ist. Im Fall von Signal ist das wirklich hilfreich, weil es sicherstellt, dass Sie sich nicht auf unser Wort für unsere Datenschutzversprechen verlassen müssen, denn wir haben eine ganze Gemeinschaft von Leuten, die unseren Code unter die Lupe nehmen, ihn testen, und wenn sie einen Fehler finden, melden sie ihn und wir beheben ihn. So entsteht eine Art Immunsystem, das uns ehrlich hält und dafür sorgt, dass wir von vielen Augen gesehen werden. Das ist der klassische Wert von Open Source. Je nach Lizenz ist Open Source letztlich eine legale Lizenzvereinbarung, und bestimmte Formen der Wiederverwendung sind erlaubt. Man kann den Code nehmen, man kann ihn abspalten, und im Fall von Signal kann man unseren gesamten Code nehmen, man kann ihn wiederverwenden, man darf ihn nur nicht Signal nennen. Open Source ist ein wesentlicher Pfeiler, um das, was wir tun, gut, rigoros und ehrlich zu tun. Aber im Fall von KI löst es nicht die Probleme des Wettbewerbs, der zentralen Kontrolle oder der Ressourcenknappheit auf dem KI-Markt.

Ganz allgemein gibt es eine wachsende Asymmetrie zwischen dem Staat und dem einzelnen. Die Regierung weiss immer mehr über mich, und ich weiss immer weniger über die Regierung. Wie ist der freie Westen in diese Situation gekommen und wie kommt er da wieder heraus?

Ich sehe, zumindest in den USA, dass wir die Überwachungsunternehmen und die Überwachungsindustrie nicht ernsthaft von der Regierung trennen können. Das haben wir mit den Snowden-Akten und den Abhörmassnahmen gesehen: Wir wissen jetzt, dass das Geschäftsmodell der Überwachungsfirmen zum Teil deshalb existieren darf, weil es der Regierung zugutekommt, einschliesslich der Geheimdienste und anderer, die, jedenfalls in den USA, die Bürger nicht in demselben Masse ausspionieren dürfen wie die Privatwirtschaft. Diese sind miteinander verflochten.

Haben Sie ein Beispiel?

Facebook hat vor kurzem private Nachrichten zwischen einer Mutter und ihrer Tochter in Nebraska herausgegeben, die dazu dienten, sie in einem Fall von illegaler Abtreibung wegen Verbrechen und Vergehen zu verurteilen – jetzt droht ihnen eine Gefängnisstrafe. Auch wenn sich die Unternehmen manchmal weigern, die Daten an die Regierung weiterzugeben, werden sie sie letztendlich doch herausgeben, wenn sie sie haben.

«Es ist wirklich wichtig, seine Privatsphäre zu schützen, bevor man sie braucht. Nicht in einem Moment der Krise.»

Meredith Whittaker

Wie kann ich am besten die Verantwortung für meine eigene digitale Sicherheit übernehmen?

Verwenden Sie Signal. Man kann auch auf lokaler Ebene Druck ausüben. Wenn Sie sehen, dass Ihre Schulen Gesichtserkennung einführen, wie es in den USA geschieht, können Sie zu einer Versammlung gehen und sich dagegen aussprechen. Wenn Sie sehen, dass Ihre Regierung im Namen der Kinderfürsorge auf Rechnungsprüfungen oder kundenseitiges Scannen drängt, können Sie sagen, dass dies ein Vorwand für Überwachung sei und wir dies nicht akzeptierten. Es ist wirklich wichtig, seine Privatsphäre zu schützen, bevor man sie braucht. Nicht in einem Moment der Krise.

Was ist mit der Verwendung von VPN oder dem TOR-Browser?

TOR ist grossartig und hilft, die Privatsphäre zu schützen, aber es ist schwer zu benutzen. Und bei VPN weiss man einfach nie, wer der VPN-Anbieter ist. Es ist ein wirklich betrügerischer Markt. Sie müssen einen vertrauenswürdigen Anbieter finden.

Wenn ich ins Visier der Regierung gerate und ein Smartphone benutze, findet sie dann nicht ohnehin alles über mich heraus? Projekte wie Pegasus müssen nur die Telefonnummer kennen, um vollständigen Zugriff zu erhalten.

Pegasus ist ein wahrlich gefährliches Spionageprogramm, und es sollte verboten werden. Aber es ist ja nicht so, dass ich Ihre Telefonnummer in einer Webseite eingeben kann und Pegasus Sie dann angreift. Es zielt auf eine einzelne Person ab, es ist kein riesiges Rasterfahndungssystem. Und es ist teuer. Ich finde es absolut verabscheuungswürdig, dass Regierungen auf der ganzen Welt, auch die US-Regierung, Lizenzen für diese Spionagetechnologien vergeben. Wir haben gesehen, wie Mexiko diese Technologie zum Ausspionieren von Journalisten eingesetzt hat.

Sie haben gesagt, wenn die EU-Kommission das Gesetz zur Chatkontrolle durchsetze, werde Signal Europa endgültig verlassen. Ist das immer noch Ihr Plan?

Wir werden niemals freiwillig gehen. Aber wenn wir vor der Wahl stehen, entweder unsere Verschlüsselung zu verfälschen, die Datenschutzversprechen zu untergraben, oder zu gehen, dann würden wir abziehen. Denn wir werden diejenigen, die sich auf uns verlassen, nicht verraten. Aber wir sind zuversichtlich, dass dieses furchtbar fehlgeleitete Gesetz korrigiert wird, bevor es dazu kommt.

Wie schätzen Sie das Risiko ein, dass die Chatkontrolle bereits auf der Ebene des Betriebssystems implementiert oder vorgeschrieben wird?

Dies würde bedeuten, dass die Betriebssysteme, auf die sich jeder verlässt, eine erhebliche Schwachstelle aufweisen. Niemand könnte diesen Systemen trauen, auch nicht die Nachrichtendienste, der Finanzsektor, die Regierung und so weiter. Das wäre eine Katastrophe.

Gibt es noch andere gefährliche Regierungsmassnahmen, vor denen sich freiheitsliebende Menschen in Europa fürchten sollten?

Die Spionageklausel im britischen Gesetz zur Online-Sicherheit ist ein weiteres Beispiel dafür. Generell sehe ich derzeit in vielen Ländern Europas, im Vereinigten Königreich, in den USA und bis zu einem gewissen Grad auch darüber hinaus eine Art religiöse Inbrunst, mit der versucht wird, sehr gefährliche Gesetze durchzusetzen, die die Ende-zu-Ende-Verschlüsselung untergraben würden. Und Ende-zu-Ende-Verschlüsselung ist natürlich der Name für die einzige Technologie, die uns zur Verfügung steht und die tatsächlich den Schutz der Privatsphäre in der zwischenmenschlichen Kommunikation gewährleistet. Das wäre also eine Katastrophe und würde letztlich die Abschaffung der zwischenmenschlichen Privatsphäre in der digitalen Welt bedeuten. Wir sollten nicht vergessen: Wir haben nicht wirklich die Wahl, ob wir Online-Tools und -Dienste nutzen wollen. Wir werden in eine Welt hineingeboren, in der wir im Wald aufwachsen, Beeren essen und keine Freunde haben können. Aber ansonsten sind wir gezwungen, diese Dienste zu nutzen, und das ist keine Frage der individuellen Entscheidung. Unser Leben, unsere Gesellschaft, unsere Regierungen, unsere Arbeitsplätze sind darauf ausgerichtet. Die Nichtnutzung sozialer Medien wird in vielen KI-Bewertungsprogrammen, die Menschen für soziale und andere Leistungen beurteilen, als Risikofaktor angeführt.

Viele sagen: «Wer nichts zu verbergen hat, hat auch nichts zu befürchten.» Was ist Ihre Antwort darauf?

Ich glaube nicht, dass viele Leute das denken, denn viele schätzen ihre Privatsphäre sehr. Wenn sie nachts mit ihrem Partner sprechen, wollen sie nicht, dass dies jemand mitbekommt. Wenn sie sich vorstellen würden, dass alles, was sie auf ihrem Alexa-Gerät sagen, plötzlich aus den Lautsprechern an ihrem Arbeitsplatz ertönt, würden sie wahrscheinlich zusammenbrechen und zu weinen beginnen. Leute sind besorgt, weil es keine individuelle Entscheidung ist, die sie treffen können, wenn sie eine Wegbeschreibung zur Arbeit benötigen, wenn sie sich in ihren Arbeitsplatzcomputer einloggen müssen und so weiter. Als die Produkte und Dienste des Internets in den 1990er-Jahren eingeführt wurden und in den 2000er-Jahren zur Infrastruktur unserer Welt wurden, wurden die Bedingungen nie klargestellt: Es wurde nicht gesagt, dass Datenbanken über ihren Standort, ihre Freunde und ihre Einkäufe geführt werden. All diese Daten werden in Zukunft verwendet, um KI-Systeme zu trainieren, die beispielsweise beurteilen sollen, ob Sie ein guter Arbeitnehmer sind oder nicht. Bei der Einführung von Online-Technologien in unser tägliches Leben wurde viel getrickst und in die Irre geführt, und wir beginnen gerade erst, die schädlichen Folgen zu erkennen. ‹

Das Interview ist auf schweizermonat.ch in Englisch verfügbar.

Meredith Whittaker
ist die Präsidentin der Messaging-App Signal.

Ronnie Grob
ist Chefredaktor dieser Zeitschrift.