
Helfen Sie mit

Wir wollen von Ihnen hören

Gemeinsam mit internationalen Medien sucht die Republik Whistleblower aus der Technologieindustrie. So können Sie sich sicher bei uns melden – eine Gebrauchsanleitung.

Von Ihrem [Expeditionsteam](#), 30.01.2019

Die Technologiebranche hat uns eine Vielzahl neuer Möglichkeiten eröffnet und unser Leben verändert. Big-Data-Unternehmen verfügen über gewaltigen Einfluss und kennen manche unserer persönlichsten Geheimnisse. Zum Teil arbeiten die Unternehmen eng mit anderen Firmen aus der Privatwirtschaft oder mit Geheimdiensten zusammen. Dabei entwickeln sie einen immer stärkeren Einfluss auf demokratische Prozesse.

In den vergangenen Jahren sind Bedenken laut geworden, dass Technologiefirmen Nutzer manipulieren, Daten missbrauchen oder auf unangemessene Weise Kinder ins Visier nehmen. Firmen und Regierungen wird vorgeworfen, mit Big Data demokratische Prozesse zu manipulieren. Technologieunternehmen sollen autoritären Regimes helfen, kritische Stimmen zu unterdrücken.

Das wirft ernsthafte Fragen auf: Wie reagieren digitale Plattformen auf die zunehmende Verbreitung von Fake News? Wie setzen sie sich gegen staatliche Einmischung zur Wehr?

In diesem Zusammenhang möchten wir Sie, liebe Leserin, lieber Leser, persönlich ansprechen: Besitzen Sie Informationen, wonach eine Technologiefirma etwas Falsches tut oder mit seinen Daten nicht korrekt umgeht? Sind Sie davon überzeugt, dass die Öffentlichkeit dadurch Schaden nimmt, dass sie ausgenutzt oder hinters Licht geführt wird?

Wollen Sie ein Schlaglicht auf einen Bereich werfen, der für unser Leben relevant ist und mit Big Data zu tun hat? Sind Ihre Informationen so wichtig, dass diese ein globales Publikum von mehr als 66 Millionen Lesern und Leserinnen in vier Sprachen (Deutsch, Englisch, Französisch, Spanisch) erreichen sollen?

Dann wollen wir von Ihnen hören – unabhängig davon, ob die fraglichen Daten in sozialen Netzwerken genutzt werden, für Marketingzwecke, im Gesundheitswesen, in der Strafverfolgung, für maschinelles Lernen, künstliche Intelligenz oder andere Zwecke. Whistleblower könnten Erkenntnisse zu gemeinhin falsch verstandenen oder fragwürdigen Praktiken beisteuern und beispielsweise erklären, warum Unternehmen sich für bestimmte Produkt-Updates entschieden haben und wie sich diese für den Verbraucher auswirken. Ein guter Hinweis basiert nicht auf Gerüchten und Spekulationen, sondern er enthält spezifische Beweise für ein Fehlverhalten.

The Signals Network

Republik, «Die Zeit» und «Zeit online», «El Mundo», «Mediapart», «The Daily Telegraph» und «The Intercept» arbeiten zusammen mit dem Signals Network, einem gemeinnützigen Unternehmen aus den USA, das zu Recherchen anregen und diese erleichtern will. Diese investigativen Recherchen sollen mithilfe von Whistleblowern die Bedeutung von Transparenz und öffentlicher Rechenschaftspflicht für die Gesellschaft hervorheben und so das öffentliche Interesse am Thema Big Data steigern.

Das Signals Network ist eine unabhängige Stiftung. Sie unterstützt Medienkooperationen, um die gesellschaftlichen Auswirkungen ihrer Rechercheergebnisse zu maximieren und ausgesuchten Whistleblowern Unterstützung zukommen zu lassen. [Mehr über das Signals Network erfahren Sie hier.](#)

Wie funktioniert die Signal-App?

Signal ist ein verschlüsselter Messenger und eine Telefon-App, die unabhängig von der Stiftung entwickelt wurde. Signal speichert Ihre Nummer, legt aber keine Logdatei zu Ihrer ein- oder ausgehenden Kommunikation an. Sie können die Software so einstellen, dass alle Botschaften, die sich nicht mehr auf Ihrem Telefon, dem Telefon des Empfängers oder in der Cloud befinden, gelöscht werden.

Hier können Sie Signal für [Android](#) oder [iPhone](#) downloaden.

Signal ist einfach zu bedienen: Öffnen Sie die App und tippen Sie auf das Stift-Symbol (auf dem iPhone; bei Android-Handys unten rechts), um eine neue Nachricht zu schreiben. Geben Sie unsere Telefonnummer (**+1 646 846 0596**) in das Suchfeld ein. Schon können Sie uns eine verschlüsselte Nachricht per Signal zukommen lassen.

Befolgen Sie [diese Empfehlungen](#), um Ihr Smartphone und die Signal-App so sicher wie möglich einzustellen.

Sie sollten nur Textnachrichten und Dokumente per Signal versenden.

Telefonanrufe werden nicht beantwortet, klassische SMS-Nachrichten werden nicht überwacht.

Wie können Whistleblower den Big-Data-Aufruf beantworten?

Wenn Sie möchten, dass Ihre Geschichte über die kombinierte Reichweite der beteiligten Medien ein globales Publikum erreicht, vergessen Sie bitte auf keinen Fall, die Worte «**Big-Data-Aufruf**» in Ihre Kontaktanfrage zu schreiben.

Die Medien des «Big-Data-Aufrufs» erreichen Sie über **die Signal-App unter: +1 646 846 0596.**

PGP-Verschlüsselung für E-Mails

Sie können uns E-Mails senden, die mit sogenannter PGP-Software (Pretty Good Privacy) verschlüsselt wurde. Verwenden Sie dazu eine PGP-Anwendung wie beispielsweise Mailvelope oder Enigmail. Damit wird der Inhalt Ihrer Nachricht verschlüsselt. Es ist für Dritte jedoch trotzdem nachvoll-

ziehbar, dass wir in Kontakt stehen. Versenden Sie deshalb Ihre Nachricht nie von Ihrer beruflichen E-Mail-Adresse, sondern – wenn möglich – von einem anonymen E-Mail-Konto. Wenn Sie uns unverschlüsselte E-Mails an die genannten Adressen senden, kann Ihre E-Mail und die Kommunikation von Dritten mitgelesen werden.

Hier können Sie unseren öffentlichen Schlüssel herunterladen und anhand des Fingerabdrucks überprüfen:

PGP Public Key: [46DA 8CB6 62C3 9B03 50B1 B769 A74A 822E A650 CA94](#)

Schicken Sie die **durch PGP verschlüsselte E-Mail an eine dieser Adressen:**

whistleblower@republik.ch

whistleblower@zeit.de

pistas@elmundo.es

lanceurdalerte@mediapart.fr

whistleblower@telegraph.co.uk

whistleblower@theintercept.com

Alle Medienpartner erhalten zeitgleich die über die Verschlüsselungs-App Signal oder über die oben genannten E-Mail-Adressen eingehenden Informationen. Journalistinnen der genannten Medien überwachen die beiden Kanäle.

Versand per Briefpost

Die ganz gewöhnliche Post kann ebenfalls eine sichere Methode sein, vor allem dann, wenn Sie Ihr Schreiben nicht in einer Post aufgeben, sondern in einen Briefkasten einwerfen.

Bedenken Sie dabei bitte, dass die amerikanische Post die Informationen aller Sendungen speichert, die durch das Postsystem versandt werden. Dazu zählt der Ort, von dem aus Sie Ihr Paket verschicken, und möglicherweise auch eine Probe Ihrer Handschrift. Sollten Strafverfolgungsbehörden Ihr Paket kontrollieren, bevor es uns erreicht, werden sie alles sehen können, was Sie uns schicken. Ausserdem bekommen sie möglicherweise Ihre Fingerabdrücke sowie in Dokumenten enthaltene Informationen, beispielsweise Tracking Dots von Druckern.

Werfen Sie Ihre Sendung ohne Absenderadresse in einen öffentlichen Briefkasten ein (nicht von zu Hause, dem Arbeitsplatz oder einem Postamt verschicken!).

Republik

Sylke Gruhnwald
Sihlhallenstrasse 1
8004 Zürich
Schweiz

Die Zeit / Zeit online

Karsten Polke-Majewski
Buceriusstrasse Eingang Speersort 1
20095 Hamburg
Deutschland

El Mundo

Rafael Moyano
Avenida de San Luis, 25
28033 Madrid
España

Mediapart

Yann Philippin
8, passage Brulon
75012 Paris
France

The Daily Telegraph

Claire Newell
111 Buckingham Palace Road
London, SW1W 0DT
United Kingdom

The Intercept

Ryan Tate
114 Fifth Avenue
New York, NY 10011
USA

An diesem Aufruf sind folgende Journalisten beteiligt:

Republik: [Adrienne Fichter](#), [Sylke Gruhnwald](#), [Patrick Recher](#)

«Die Zeit»: [Holger Stark](#), [Karsten Polke-Majewski](#), [Sascha Venohr](#), [Kai Biermann](#), [Yassin Musharbash](#)

«El Mundo»: [Paula Guisado](#)

«Mediapart»: [Yann Philippin](#), [Fabrice Arf](#)

«The Daily Telegraph»: [Claire Newell](#)

«The Intercept»: [Ryan Tate](#), [Sam Biddle](#), [Micah Lee](#)

Zur Recherche Kooperation

Alles über die internationale Kooperation der Republik mit der Stiftung The Signals Network und fünf weiteren Medienunternehmen [erfahren Sie hier](#).