Donnerstag, 23. Januar 2020, 16:00 Uhr
~17 Minuten Lesezeit

Informelle Selbstverteidigung im Netz

Am 17. September 2019 ist Edward Snowdens Autobiographie „Permanent Record“ erschienen. Conrad Knittel fasst die Kernaussagen zusammen. Teil 3/3.

von Conrad Knittel
Foto: PopTika/Shutterstock

Über die Bespitzelung zu klagen, reicht nicht. Und da nicht alle so ohne weiteres auf Notebook und Smartphone verzichten können, stellt sich die Frage, ob man dem digitalen Big Brother etwas entgegensetzen kann. Der Whistleblower Edward Snowden gibt Tipps, wie wir im Internet unsere Privatsphäre schützen können. Der Autor erweitert die Perspektive und leitet daraus konkrete Handlungsempfehlungen ab. Zum neuen Jahr könnten wir uns vornehmen, etwas davon umzusetzen.

In den ersten beiden Artikeln dieser Reihe habe ich Snowdens Werdegang (https://www.rubikon.news/artikel/der-enthullungsthriller) und seine Beweggründe (https://www.rubikon.news/artikel/snowdens-appell) dargestellt. In diesem dritten und abschließenden Artikel werde ich auf seine Empfehlungen eingehen, wie wir uns individuell gegen Massenüberwachung wehren können.

Was ist unser Ideal?

Zunächst sollten wir uns klar darüber werden, was wir überhaupt erreichen wollen. Was bedeutet der Schutz unserer Privatsphäre im Internet? Ich schlage vor, dass wir darunter verstehen, so weitreichend wie möglich anonym zu bleiben. Ich würde noch einen Schritt weitergehen und von *Datensparsamkeit* sprechen, also der Idee, dass möglichst wenig Daten über meine Aktivitäten im Internet entstehen, gesammelt und gespeichert werden.

Denn selbst wenn diese Daten anonym gesammelt würden, also nicht mit mir als Person verknüpft wären, bliebe das Problem, dass — soziologisch betrachtet — noch immer die gleiche Datenflut zur Möglichkeit der Manipulierbarkeit und Überwachung der Bevölkerung bliebe. Außerdem lässt sich theoretisch eine ausreichend komplexe Menge an Daten wieder der Person zuordnen, von der sie ausgeht (1).

„Möglichst wenig Daten über meine Aktivitäten“ hieße im Grenzfall: gar keine. Dieses Ideal werden wir — wie sich zeigen wird — nicht erreichen können, aber es lohnt sich trotzdem, es zur Orientierung vor Augen zu behalten.

Wir brauchen die aktive Auseinandersetzung

Die meisten Regierungen und Unternehmen verfolgen jedoch — systemisch bedingt — das genau gegenteilige Ideal, wenn man denn von einem Ideal sprechen möchte. Sie profitieren im Allgemeinen von möglichst wenig Anonymität und geringer Datensparsamkeit der Bürger — als Wähler und Untertanen — respektive Kunden — als Konsumenten und Fans.

Das Geschäftsmodell vieler großer Internetfirmen basiert geradezu auf *Datenreichtum* (2). Nur dadurch können sie viele ihrer Dienstleistungen kostenlos anbieten, was viele Nutzer für einen großen Vorteil des Internetzeitalters halten — ob zu Recht oder Unrecht, sei dahingestellt, weil die Frage äußerst komplex ist.

> ***Das bedeutet, dass wir mit unserem Ideal von Anonymität und Datensparsamkeit gegen die Interessen derjenigen Entitäten vorgehen, die meines Erachtens am meisten Einfluss und Macht in unseren***

> ***Gesellschaften haben.***

Dadurch wird die Angelegenheit nicht gerade erleichtert, aber andererseits bietet sich uns hier eine hervorragende Gelegenheit, unsere Entschlossenheit zu erproben.

Snowden zufolge gibt es Grund zur Hoffnung. Wenn genug Menschen sich nicht damit begnügten, das Problem zur Kenntnis zu nehmen, aber in Passivität zu verharren, ließe sich aktiv daran arbeiten, die angemessene Privatsphäre im Internet wiederherzustellen. 2016 sei zum ersten Mal mehr Internetverkehr verschlüsselt gewesen als unverschlüsselt (3).

Zudem gebe es mit Techniken wie TOR, Programmen wie Signal und Betriebssystemen wie TAILS immer bessere und ausgefeiltere Werkzeuge, um sich der Überwachung zu widersetzen. Auf diese Werkzeuge werde ich noch eingehen. Zuvor will ich aber die Entwicklungen darstellen, die laut Snowden eher zu mehr Datenreichtum und Überwachung führen werden, wenn wir den Fehler begehen sie zu nutzen.

Fehler 1: Das Internet der Dinge

Das sogenannte „Internet der Dinge“ sei auf Datenreichtum ausgelegt. Snowden beschreibt in seinem Buch, wie ihm dies klar wurde, als er zum ersten Mal einen „Smartfridge“, einen internetfähigen Kühlschrank, sah. Dieser verfügte über einen Bildschirm, sodass man ihn wie einen Computer benutzen konnte: E-Mails lesen, YouTube et cetera. Zusätzlich kontrolliere der Kühlschrank per Strichcode die Haltbarkeit der vorhandenen Lebensmittel, habe ihm der begeisterte Verkäufer erklärt (4). Das alles für schlappe 9000 Dollar. „Das war nicht ganz die umwerfend innovative Hightech-Zukunft, die man uns versprochen hatte“,

schreibt Snowden.

„*Dass der Kühlschrank internetfähig war, diente, davon war ich überzeugt, nur dem einen Zweck, den Hersteller über die Nutzungsgewohnheiten seiner Besitzer und andere Haushaltsdaten in Kenntnis zu setzen. Der Hersteller seinerseits würde diese Daten dann zu Geld machen, indem er sie weiterverkaufte. Und wir sollten für dieses Privileg noch bezahlen.*“

Alles, was über Sensoren und eine Verbindung zum Internet verfügt, kann dazu genutzt werden, uns auszuspähen — ob es die Smartwatch ist, das Smartphone, Alexa und Siri — oder natürlich auch unser Computer. Das ist, wie Snowden ausführt, die Logik der technischen Möglichkeiten: Was möglich ist, wird — früher oder später, aber meist eher früher — auch gemacht.

Ich würde hinzufügen: Es ist auch die Logik des Marktes, nicht unbedingt die Logik der menschlichen Würde. Ich will dabei keine bösen Absichten unterstellen. Im Gegenteil, es folgt ja einer Logik, nur nicht der, die ich bevorzugen würde. Man sollte sich gründlich fragen, warum man denn überhaupt wollen sollte, dass der eigene Kühlschrank intelligent wird oder das Auto oder das T-Shirt (5).

Fehler 2: Die Cloud

Die Idee der „Cloud“, wie ich sie verstehe, ist die, dass der Benutzer seine Daten auf einen oder mehrere Server hochlädt. Das hat folgende Vorteile: Erstens dient sie als Backup, sollte das eigene Gerät einmal den Geist aufgeben, zweitens kann überall auf sie zugegriffen werden und drittens müssen keine Daten mehr auf dem eigenen Gerät gespeichert werden (6). Dies kann Vorteile haben, meines Erachtens allerdings eher für Firmen oder Organisationen und ihre Mitarbeiter als für Privatnutzer.

> ***Leider, so Snowden, seien Privatnutzer in der Regel aber so begeistert von der Idee, ihre Fotos, Videos und Musik global zu speichern, dass sie sich gar nicht die Frage stellten, warum ihnen dieser Service so gut wie kostenlos angeboten wird.***

Das Problem aus der Perspektive der Datensicherheit sei aber, dass deine hochgeladenen Daten dir nicht mehr so richtig gehörten, sondern jetzt von Firmen kontrolliert würden, die damit im Grunde machen könnten, was sie wollen (7).

Die Gemeinsamkeit beider Fehler scheint mir zu sein, dass sie auf Bequemlichkeit und Verführung beruhen. Beide Techniken versprechen uns, unsere Lebensqualität deutlich zu erhöhen, was ohnehin fraglich ist, und setzen auf die Bequemlichkeit der Nutzer, die diese Geschäftspraktiken wiederum nicht überprüfen. Man könnte mit **Erich Fromm** (https://de.wikipedia.org/wiki/Haben_oder_Sein) sagen, beide ziehen uns mehr Richtung Haben-Lebensweise als Seins-Lebensweise (8).

Anonymität

Nehmen wir nun an, wir haben uns nicht verführen lassen, haben keinen internetfähigen Kühlschrank, keine Alexa oder Ähnliches und unsere Daten nicht auf Facebook und in die Cloud hochgeladen. Dann bleiben immer noch die Geräte, ohne die man als Normalsterblicher heutzutage weder sozial noch beruflich leben kann: Smartphone und Computer. Auf diese beiden Geräte sollte man sich beschränken, wenn man es ernst meint mit der Privatsphäre (9).

Leider sind diese beiden Geräte nicht von Natur aus sicher und es bedarf eines gewissen Aufwands an Zeit, Energie und gegebenenfalls

auch Geld, um hier nachzubessern. Allerdings ist dies immerhin möglich — anders als beim „Smartfridge“.

Zunächst sei nun die einfache Regel formuliert, dass wir unsere Identität nicht selbst preisgeben sollten. Wir tun dies aber, sobald wir uns mit echtem oder auch nur ähnlichem Namen bei Facebook anmelden oder unsere E-Mails checken, wenn wir uns bei Amazon oder PayPal einloggen et cetera. Warum muss dies überhaupt erwähnt werden? Weil wir dazu tendieren, es zu vergessen. Snowden schildert, wie selbst beim CIA immer wieder der Fehler gemacht wurde, dass Mitarbeiter sich in der gleichen Internetsession, in der sie eine Tarnfirma benutzten, bei Facebook einloggten — und in ihrem Account angegeben hatten, dass sie für die CIA arbeiteten.

Verschlüsselte Kommunikation

Bei all unserer Kommunikation sollten wir Wert auf Ende-zu-Ende-Verschlüsselung legen. Verschlüsselung ist laut Snowden, das beste Mittel, um uns gegen Überwachung jeglicher Art zu wehren. Was heißt nun Ende-zu-Ende-Verschlüsselung und warum ist sie so wichtig? Es heißt, dass deine Kommunikation auf deinem Gerät mit einem Schlüssel versehen wird und für andere, die den Schlüssel nicht haben, unlesbar wird. Denn nur du und der Empfänger haben diesen Schlüssel. Die Kommunikation wird erst beim Empfänger wieder entschlüsselt (10). Die Kommunikation bleibt die gesamte Zeit, die sie im Internet verbringt, verschlüsselt und kann daher theoretisch nicht mitgelesen oder -gehört werden. Wir sollten jedoch im Hinterkopf behalten, dass auch bei verschlüsselter Kommunikation noch Metadaten anfallen.

Die meiste private digitale Kommunikation findet heutzutage über Messenger statt, außerdem über E-Mails und Internettelefonie. Die

gute Nachricht ist, dass die allermeisten Messenger-Anbieter mittlerweile standardmäßig eine solche Verschlüsselung anbieten, zum Beispiel auch „WhatsApp“. Dennoch empfiehlt Snowden den Messenger „Signal“ und auch die Internetseite **prism-break.org** (https://prism-break.org/en/) spricht sich für „Signal“ oder „Conversations“ aus.

„Signal“ funktioniert sehr ähnlich wie „WhatsApp“, hat aber ein paar Vorteile. Erstens ist es nicht im Besitz eines riesigen Unternehmens, dessen Geschäftsstrategie darauf ausgelegt ist, Datenreichtum zu generieren. Zweitens ist die Software „open source“, was bedeutet, dass auch **öffentlich überprüft werden kann** (https://www.infoworld.com/article/2985242/why-is-open-source-software-more-secure.html), inwiefern sie keine sogenannten **„backdoors“** (https://de.wikipedia.org/wiki/Backdoor) oder schwerwiegende Sicherheitsprobleme enthält. Drittens speichert „Signal“ ein **Minimum an Metadaten** (https://netzpolitik.org/2016/nun-amtlich-der-messenger-signal-ist-ziemlich-sicher/), die — wir erinnern uns — das hauptsächliche Interesse der Geheimdienste auf sich ziehen (11). Außerdem kann über „Signal“ auch verschlüsselt telefoniert werden.

„Conversations“ ist meines Erachtens noch empfehlenswerter, weil es noch weniger Daten des Nutzers erhebt, insbesondere weder die eigene noch fremde Telefonnummern. Es ist jedoch auch etwas mehr Aufwand, es einzurichten, dafür kann man es über einen eigenen Server laufen lassen — wenn man weiß, wie das geht. Ich würde — pace Snowden — am ehesten „Conversations“ empfehlen.

Beide Messenger haben leider einen wichtigen Nachteil: Sie sind weniger verbreitet als „WhatsApp“. Sich vollkommen von Letzterem zu verabschieden, hieße, Kontakte zu verlieren und neue Kontaktmöglichkeiten zu verkomplizieren. Meiner persönlichen Erfahrung nach ist es nicht einfach, andere für die Idee zu

gewinnen, verschiedene Messenger auszuprobieren. Woran mag dies liegen?

„Gib einfach alles der Datenkrake.“

Ich vermute, ein ganz großes Problem ist, dass wir überhaupt kein direktes Feedback erleben — weder, wenn wir versuchen uns anonymer im Internet zu bewegen, noch bei normalem Konsum. Wir können ja nicht sehen, wie sichtbar wir sind, sondern müssen uns gewissermaßen darauf verlassen, dass dem wohl so oder so sein wird. Dadurch verlieren wir dieses Thema dann aber auch schnell wieder aus dem Blick.

Ein weiteres Problem ist eine Art Resignation, die sich darin ausdrückt, dass viele Menschen davon ausgehen, dass Google sowieso alles über sie weiß. Als ich anfing, ein Smartphone zu benutzen und mich fragte, wie ich meine ganzen persönlichen Daten von einem Gerät auf das nächste übertragen sollte, ohne dass dies unendlich viel Zeit in Anspruch nehmen würde, riet man mir: „Gib einfach alles der Datenkrake.“

Verschlüsselte E-Mails, Linux und TAILS

Beim Thema E-Mails ist es leichter, weil es keine Rolle spielt, ob man den gleichen Anbieter hat. Wichtig ist hier, wie auch bei anderen Angeboten, zu prüfen, ob der eigene Anbieter eine solide Verschlüsselung gewährleistet. Auf **prism-break.org** (https://prism-break.org/en/) finden sich Empfehlungen, ebenso auf **dieser Seite.** (https://prxbx.com/email/).

Es bringt leider nicht viel, meine Nachrichten auf dem Gerät zu verschlüsseln, wenn die Aktivitäten auf dem Gerät selbst schon

mitgeschnitten werden können. Auch davon abgesehen tendieren die gängigen Betriebssysteme leider nicht zur Datensparsamkeit. Dein Standard-Android will einen Google-Account, dein Windows ein Microsoft-Konto — natürlich beides mit deinem echten Namen. Bei Apple ist es genauso. Was bleibt?

Gehen wir zuerst auf den Computer ein, weil es hier einfacher ist. Mit Windows oder MacOS werden wir unser Ziel nicht so leicht erreichen. Einfacher ist es, eine Linux-Variante zu benutzen. Für den Anfang ist es fast egal, welches Linux wir nehmen, man empfahl mir einfach UBUNTU. Auf **prism-break.org** (https://prism-break.org/en/) können detailliertere Empfehlungen gefunden werden. UBUNTU sieht fast so aus wie Windows und funktioniert hinreichend ähnlich, sodass es für die allermeisten Computernutzer kein Problem darstellt zu wechseln. Im Internet findet sich jede Hilfe, die man benötigen könnte.

Eine weitere Möglichkeit, sich mit Linux schnell auseinanderzusetzen, ist die Distribution TAILS, die Snowden auch selbst benutzt hat, um anonym ins Internet zu gehen. Er nutzte hierbei allerdings auch fremde WLAN-Zugänge, was ein weiterer Schritt in Richtung Anonymität ist und was wir über **Freifunk** (https://freifunk.net/) legal nachmachen können. TAILS kann **kostenlos aus dem Internet bezogen** (https://tails.boum.org/install/index.de.html), auf DVD oder USB-Stick gespeichert und von diesem Medium aus auf jedem Computer ausgeführt werden.

TOR

TAILS hat einen TOR-Browser eingebaut, den Snowden ebenfalls empfiehlt. „Tor ist eine freie Open-Source-Software, die ihren Nutzern bei sorgfältiger Anwendung praktisch in sämtlichen

Kontexten völlig anonyme Online-Recherchen erlaubt.“ Das klingt doch schon mal gut. Allerdings sollten wir im Hinterkopf behalten, dass wir nicht anonym bleiben, wenn wir uns irgendwo mit annähernd echten Personaldaten einloggen. Es ist weiterhin sichtbar, dass wir das Internet nutzen, insbesondere auch, dass wir TOR nutzen — denn Metadaten fallen an —, lediglich nicht mehr, was genau wir tun, zumindest wenn alles gut geht. Auch dieses Problem kann gelöst werden, indem eine sogenannte **verschleierte Bridge** (https://tails.boum.org/doc/first_steps/startup_options/bridge_mode/index.de.html) verwendet wird, hierfür benötigt man jedoch etwas mehr Know-how als ein Amateur.

TOR-Browser gibt es auch unabhängig von TAILS und Linux. Um ansatzweise zu erklären, wie das TOR-Projekt funktioniert, gehe ich kurz darauf ein, wie das Browsen im Internet normalerweise funktioniert. Wenn ich in meinem Browser eine URL eingebe oder über Google etwas suche — was die beiden gängigsten Suchmethoden sind —, dann läuft eine Suchanfrage von mir zu einem Server und diese enthält nebst vielen anderen Daten die Information, wohin die angeforderte Information zurückgesendet werden soll: zu mir. Dadurch bin ich als Ausgangspunkt der Anfrage nicht anonym.

Nutze ich TOR, dann läuft meine Suchanfrage nicht direkt zum anvisierten Server, sondern über mehrere zwischengeschaltete Server. Jeder Server kennt nur zwei andere Server: den, von dem er die Anfrage erhielt und den, an den er sie weiterleitet. Dadurch weiß der letzte Server, an den die Suchanfrage ging, nicht mehr, dass die Informationen zu mir gelangen werden. Das Prinzip erinnert an Zwiebelschalen, daher auch der Name: The Onion Router (12).

Smartphones sind nicht sicher

Verwende ich auf meinem Laptop TAILS und TOR und verrate mich nicht selbst durch das Einloggen in Accounts, die zu mir verfolgt werden können — im Idealfall gehe ich noch von einem Internetanschluss aus, der nicht auf mich registriert ist — dann bin ich schon recht sicher unterwegs, was meine Daten angeht. Auf dem Smartphone eine ähnliche Anonymität zu schaffen, ist zum aktuellen Zeitpunkt sehr viel komplizierter und für den Laien kaum zu bewältigen. Zu diesem Thema hat auch Snowden in seinem Buch nichts geschrieben.

Das größte Problem scheint zu sein, dass es mit den vorinstallierten Betriebssystemen Android und iOS nicht praktikabel ist, ohne einen Google- oder Apple-Account auszukommen. Ein weiteres Problem sind die SIM-Karten selbst, aber auch der WLAN-Zugang, die nicht physisch deaktivierbaren Sensoren — GPS, Kamera, Mikro —, eigentlich fast alles, was das Gerät ausmacht. Zusätzlich bedeutet jede App, die man installiert, ein Sicherheitsrisiko — was nebenbei auch für Programme auf dem Computer gilt.

Ich habe mir sagen lassen, dass die möglichen Alternativen eine starke Einschränkung der Nutzbarkeit beinhalten. Empfohlen wurden mir einerseits freie Android-Versionen wie „Replicant“ und „LineageOS“ sowie „Librem 5“, ein mit Fokus auf Sicherheit und Privatsphäre designtes Smartphone.

Allerdings laufen die meisten Apps — wenn überhaupt — in diesen Umgebungen nicht ohne Probleme. Daher habe ich mich bisher nicht an diesen Schritt herangetraut und kann nichts Wesentliches dazu sagen. Diskussionen im Internet findet man, aber sie scheinen keinen roten Faden zu ergeben. Dieses Feld wird sich sicherlich im Lauf der Zeit weiterentwickeln (13).

Umsetzung

Fassen wir zusammen:

> ***Um meine Privatsphäre bestmöglich zu schützen, verwende ich so wenig internetfähige Technologie so selten wie möglich. Ich lasse die Finger vom Internet der Dinge. Ich lade meine Daten nicht in die Cloud. Ich lade meine Daten nicht in soziale Netzwerke. Ich verwende nicht meinen richtigen Namen im Internet.***

Ich logge mich so wenig wie möglich ein. Ich logge mich direkt wieder aus. Ich starte nach einem Login eine neue Internetsession, wenn ich anonym sein will. Ich verwende nur Kommunikationsdienste mit Ende-zu-Ende-Verschlüsselung. Ich bin vorsichtig im Umgang mit kostenlosen Services, denn wenn etwas kostenlos ist, dann sind die Kosten nur versteckt. Irgendwer zahlt und in den meisten Fällen nicht aus Nächstenliebe, sondern für unsere Daten.

Im nächsten Schritt verabschiede ich mich von datenreichen Unternehmen und wechsle zu Open-Source-Software (14). Ich verwende Linux und TOR. Dieser Schritt funktioniert bisher vor allem gut auf dem Computer, also erledige ich so viel Kommunikation wie möglich über diesen und meide das weniger sichere Smartphone.

Bin ich auf den Geschmack gekommen, kann ich daran mitarbeiten, auch das Smartphone sicherer zu machen, indem ich ein freies Android ausprobiere oder „Librem 5“ teste.

Die Umsetzung ist interessanter und fällt leichter, indem ich einerseits mit Freunden und andererseits mit Gleichgesinnten und Technikaffinen über diese Thematik kommuniziere. Die meisten Menschen — mich eingeschlossen — wissen erstaunlich wenig über das Thema Privatsphäre im Internet. Lernen wir dazu und seien wir experimentierfreudig!

Quellen und Anmerkungen:

(1) Was bedeuten würde, dass sie eben nicht wirklich hinreichend anonymisiert ist. Diese Problematik betrifft viele Bereiche, beispielsweise die Datenerfassung in medizinischen Studien, die ebenfalls anonymisiert verlaufen sollte.
(2) Den Begriff Datenreichtum habe ich von **Fefes Blog** (https://blog.fefe.de/?ts=a38e35fa) übernommen. Mir gefällt der Begriff, weil er sowohl die Akkumulation als auch die Gier danach und die damit verbundene Macht konnotiert. Man kann ihn allerdings polemisch finden und darf ihn dann mental gerne durch einen neutraleren ersetzen.
(3) Snowden meint damit wahrscheinlich das verstärkte Browsen über HTTPS statt HTTP. Man wies mich darauf hin, dass die meisten Browser dann trotzdem genug Daten vor der Verschlüsselung an die Hersteller senden und zwar aufgrund diverser Add-Ons, OCSP oder Google Safe Browsing.
(4) Edward Snowden, Permanent Record, Verlag S. Fischer 2019, Seite 244. Die Geschichte scheint so nicht ganz stimmen zu können, da von einem normalen Produkt-Strichcode nicht das Haltbarkeitsdatum abzulesen wäre. Entweder erinnert sich Snowden falsch oder der Verkäufer hat es falsch dargestellt oder Strichcodes funktionieren in den USA fundamental anders als in Deutschland. Vielleicht war gemeint, dass der Kühlschrank per Strichcodes einen Überblick über sein Inventar behält. Ich weiß es nicht.
(5) Bei dieser gedanklichen Auseinandersetzung kann natürlich auch herauskommen, dass man es will. Auf das Internet der Dinge bin ich bereits **in anderem Kontext** (https://www.rubikon.news/artikel/unsichtbare-gefahr) kritisch eingegangen. Es scheint mir immer mehr der Fall zu sein, dass es keine Perspektive gibt, aus der heraus diese Entwicklung wünschenswert wäre, mit Ausnahme der auf wirtschaftlichen

Umsatz bezogenen. Ich könnte mich irren und wäre an überzeugenden Argumenten der Gegenansicht durchaus interessiert.
(6) Bei drittens entfällt die Funktion des Backups, insofern die Version in der Cloud dann die einzige ist und eben nicht nur ein Backup.
(7) Wer dies nicht glaubt, dem empfiehlt Snowden einen Blick in die Benutzungsordnungen der „Clouds“. Die Frage ist eine rechtliche und unterliegt möglicherweise verschiedenen Gesetzgebungen. **Dieser Artikel** (https://automationspraxis.industrie.de/allgemein/kontrollverlust-in-der-wolke-wem-gehoeren-die-daten/) betrachtet die Frage aus deutscher Perspektive.
(8) Ich tätige diese Aussagen aus tiefer und reflektierter Überzeugung, kann sie aber nicht belegen. Mir scheint bei unvoreingenommener Betrachtung, dass die meisten technischen Errungenschaften eher abhängig machen und einen damit der Erfahrung berauben, etwas aus den eigenen Fähigkeiten heraus erreicht zu haben — was meiner subjektiven Erfahrung nach aber eines der schönsten Erlebnisse ist, das ein Mensch überhaupt haben kann. Andererseits setzt Technik in der Regel auch Zeit frei, die anderweitig genutzt werden kann: Wenn ich mich dank Navi seltener verfahre, verwende ich weniger Zeit auf unproduktives Autofahren. Nur nutze ich diese Zeit dann auch für etwas, was mir wirklich am Herzen liegt, zum Beispiel eine Wanderung mit Hilfe des **Wegkrokis** (https://www.scout-o-wiki.de/index.php/Wegkroki) oder daddel ich nur noch mehr rum und lasse meine Fähigkeiten, mich zu orientieren, verkümmern?
(9) Streng genommen sollte man sich auf den Computer beschränken und noch strenger genommen sollte man diesen nicht internetfähig machen. Aber bei so viel Strenge bleibt der Realismus auf der Strecke. Nur Smartphone und Computer ist meines Erachtens aber realistisch.
(10) Dies stimmt nur für den Fall der symmetrischen Verschlüsselung. Es gibt darüber hinaus asymmetrische

Verschlüsselung. Dieses Detail spielt in diesem Kontext erst einmal keine Rolle.
(11) Dennoch findet sich im Internet auch Kritik an Signal, beispielsweise die Nutzung der Handynummer, die Einbindung von Software von Drittanbietern, und dass man es nicht kompatibel über einen eigenen Server laufen lassen könne. Zudem bedeutet die Tatsache, dass Signal wenig Metadaten speichert, nicht, dass auch wenige anfallen. Mir selbst ist zudem aufgefallen, dass Signal manchmal meine Nachrichten meinem Gesprächspartner in chaotischer Reihenfolge anzeigt, was schon zu äußerst amüsanten Rekombinationen geführt hat. (Der Kreative freut sich, der Kognitive wechselt zurück zu WhatsApp.)
(12) The Intercept (Englisch) hatte vor ein paar Jahren **einen ziemlich guten Artikel** (https://theintercept.com/2015/07/14/communicating-secret-watched/) über dieses Thema.
(13) Für diesbezügliche Hinweise wäre ich dankbar.
(14) Diese Empfehlung scheint auf den ersten Blick der zu widersprechen, mich vor kostenlosen Diensten in Acht zu nehmen. Allerdings heißt „open source“ nicht automatisch, dass der Dienst kostenlos ist, sondern, dass der Quellcode frei zugänglich ist. Tatsächlich ist auch Open-Source-Software nur dann wirklich empfehlenswert, wenn transparent ist, wer aus welchen Motiven diese Software entwickelt.

Dieser Artikel erschien bereits auf www.rubikon.news.

Conrad Knittel, Jahrgang 1988, studierte Philosophie und Anglistik in Heidelberg. Nach einem kurzen

Intermezzo als Gymnasiallehrer promoviert er nun über philosophische Betrachtungen zur Evolutionsbiologie. Nebenbei schreibt er seit Jahren an einem Roman, nimmt an einer Yogalehrerausbildung und einer Kommunikationsausbildung teil und beschäftigt sich mit gesellschaftspolitischen Fragen.

Dieses Werk ist unter einer **Creative Commons-Lizenz** (**Namensnennung - Nicht kommerziell - Keine Bearbeitungen 4.0 International** (https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de)) lizenziert. Unter Einhaltung der Lizenzbedingungen dürfen Sie es verbreiten und vervielfältigen.