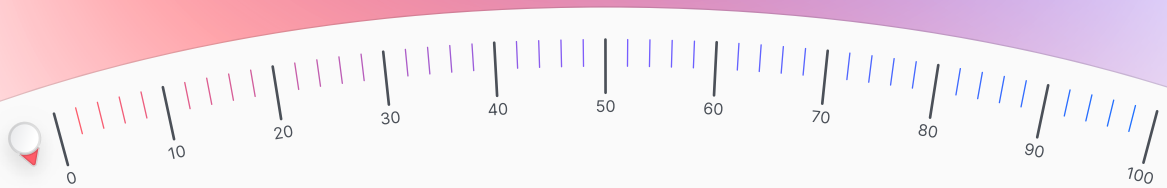
Privacy Guide

Wie können Sie Ihre Privatsphäre im Internet schützen?

Qwant, Proton, Olvid und Murena geben Ihnen die Schlüssel zum Verständnis und zur Umsetzung von Lösungen, mit denen Sie Ihre persönlichen Daten im Internet schützen können.



Anleitung zur Verfügung gestellt von:

Qwant Proton Olvid murena

Im Zeitalter einer ethischeren und verantwortungsvolleren digitalen Welt geben Ihnen **Qwant, Proton, Olvid und Murena**, die wichtigsten Akteure in Europa, die **ethische digitale Dienste** anbieten, ohne persönliche Daten zu sammeln, die Schlüssel zum **Verständnis, warum Sie Ihre Privatsphäre im Internet schützen sollten und wie Sie Ihre Daten wirklich privat halten können**. Definitionen, Ratschläge und Lösungen - dies ist DIE Anleitung, die Sie bei Ihrem Übergang begleiten wird, in eine Welt, in der Sie frei und unerkannt sind.

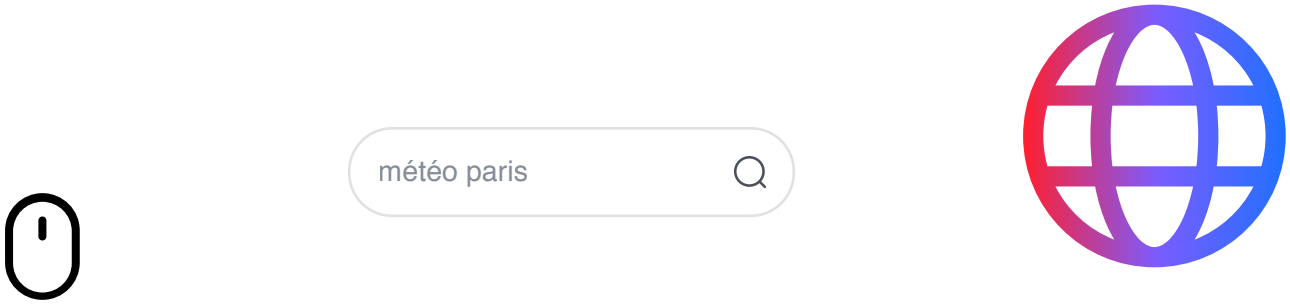
Haben Sie schon einmal das Gefühl gehabt, dass Sie beim Betreten einer Website automatisch Cookies akzeptieren? Sind Sie es leid, immer wieder Werbung für Turnschuhe zu finden, unter dem Vorwand, dass dies der Gegenstand Ihrer letzten Suche war? Akzeptieren Sie systematisch die Weitergabe Ihres Geostandorts, auch wenn die Website oder Anwendung dies nicht erfordert? Sie sind es leid, keine andere Wahl zu haben, als E-Mails, Dateien und private Informationen mit Unternehmen zu teilen, und möchten die Kontrolle über Ihre Online-Identität zurückgewinnen? Haben Sie das Gefühl, dass Ihr Smartphone Ihnen zuhört?

Wenn Sie sich in mindestens einer dieser Situationen wiedererkennen, dann ist **diese Anleitung genau das Richtige für Sie**! Wir geben Ihnen die Schlüssel, um besser zu verstehen, durch welchen Mechanismus das Internet alles über Sie weiß. Wir werden Ihnen auch **Tipps und Lösungen** geben, wie Sie die Spuren, die Sie beim Surfen im Internet hinterlassen, minimieren können.

1 Wir überarbeiten, wir lernen die Grundlagen

Bei jeder Ihrer Verbindungen im Internet hinterlassen Sie eine Spur: Gesuchte Informationen, gekaufte Produkte, gepostete Kommentare, gesendete E-Mails, kommentierte Beiträge, Logins auf Websites, Nutzung einer App - alles wird protokolliert! Das mag Ihnen vielleicht harmlos erscheinen, denn es spielt keine Rolle, dass wir wissen, was Ihnen gefällt. **Aber was ist mit den Daten, die unbeabsichtigt übermittelt werden?** Wie werden sie von den Webseiten verwendet?

Wenn Sie sich einloggen oder Anwendungen von Drittanbietern nutzen, werden diese Daten gesammelt und bilden Ihr **digitales Profil**. Ihr digitales Profil offenbart Ihre Beziehungen, Ihre Meinungen, Ihre Gewohnheiten, Ihre Bewegungen - Ihr gesamtes Privatleben. Dieses digitale Profil wird häufig an verschiedene Unternehmen verkauft und weiterverkauft, die damit Profit machen. Wie ist das möglich? Wie funktioniert das? Hier sind einige Erklärungen, die Ihnen helfen werden, das Thema besser zu verstehen.



Was ist der Unterschied zwischen einem Browser und einer Suchmaschine?

Ein Browser ist eine Software, mit der Sie Webseiten aufrufen können, z. B. eine E-Commerce-Website oder die Ihrer Lieblingsmedien. Heute sind Firefox, Safari oder Chrome die meistgenutzten Browser auf dem Markt.

Die Suchleiste des Browsers ermöglicht sowohl den Zugriff auf eine Webseite über ihre URL (*www.exemple.com*) als auch die Suche über eine Suchmaschine, die standardmäßig im Browser eingestellt ist.

Eine **Suchmaschine ist eine Website, die es ermöglicht, nach anderen Websites zu suchen**. Man greift also über einen Browser auf eine Suchmaschine zu.

Heute sind die am häufigsten verwendeten Suchmaschinen Bing, DuckDuckGo, Ecosia, Google, Lilo, Qwant oder Yahoo.

Sie stellen eine Suchanfrage, z. B. "Wetter in Paris", und die Suchmaschine wird Ihnen mehrere Webseiten vorschlagen, die Ihre Anfrage beantworten könnten.

Die Suchmaschine führt Sie zur richtigen Website, während der Browser nur eine Verbindung zur digitalen Welt darstellt.

Um den Unterschied zwischen diesen beiden Begriffen zu verdeutlichen: Der Browser ist das Fahrzeug, das Sie transportiert, während die Suchmaschine das GPS ist, das Ihnen den besten Weg zu der besten Webseite zeigt, die Ihrer Anfrage entspricht.

Was ist ein cookie ?

Sicher haben Sie schon einmal eine Werbung in sozialen Netzwerken gesehen und sich gefragt: "Wie können die wissen, dass ich dieses Produkt bereits auf einer anderen Website gesucht habe?" Die Antwort auf diese Frage lautet ... "dank" Cookies!

→ **Aber was ist ein Cookie?**

IEs ist eine kleine Textdatei, die vom Browser, auf Ihrem Computer abgelegt wird, wenn Sie eine Website besuchen. Dieses Cookie wird Ihr Surfen im Internet nachverfolgen. Dieses Cookie hat ein Verfallsdatum, d. h., es wird nach einer bestimmten Zeit gelöscht.

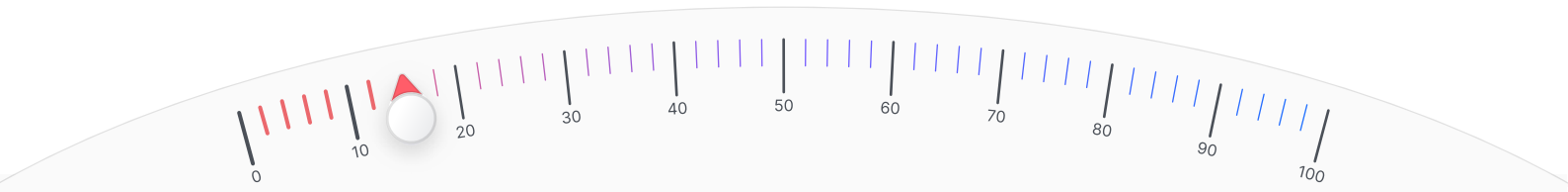
Dieses Cookie, das auf Ihrem Computer abgelegt wird, kann mehrere Zwecke erfüllen:

Funktionale Cookies:

Sie speichern Ihre Präferenzen auf einer Website, d. h. automatische Anmeldung im Konto, Standort, Sprache und andere gewählte Einstellungen. Dadurch wird Ihre Erfahrung als Nutzer einer Website verbessert.

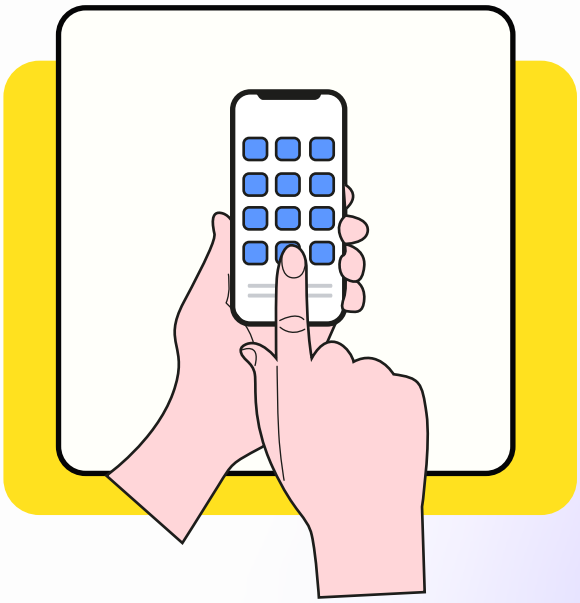
Cookies von Drittanbietern oder Werbe-Cookies:

Sie zeichnen hauptsächlich das Nutzerverhalten und den Weg des Besuchers im Internet auf, um später **ein Nutzerprofil** zu erstellen, das mit jedem Login erweitert wird. Auf der Grundlage dieses Nutzerprofils ist es dann möglich, persönliche Werbung zu platzieren. Dieses Nutzerprofil kann dann **an Drittseiten weiterverkauft werden** und z. B. soziale Netzwerke, die Ihnen später Werbung für Marken oder Produkte präsentieren, nach denen Sie zuvor gesucht haben. Auf diese Weise erhalten Sie Werbung für ein Paar Schuhe, nach denen Sie vor ein paar Tagen oder Wochen gesucht haben, ohne dass Sie jemanden gefragt haben.



Was ist ein Tracker?

Hier geht es um die Tracker, die Sie **in mobilen Apps** finden, die Sie auf Ihr Smartphone herunterladen. Diese Tracker sind Code-Bibliotheken (sog. Software Development Kit oder SDK), die dafür zuständig sind, **Informationen zu sammeln** über die Person, die eine Anwendung nutzt, oder darüber, wie diese Person die Anwendung nutzt oder in welcher Umgebung sie sich aufhält. Diese SDKs sparen Zeit bei der Entwicklung einer Anwendung, indem sie bereits vorhandenen Code verwenden. Sie können verwendet werden, um das Publikum oder den Weg, den der Nutzer in der Anwendung zurückgelegt hat, zu analysieren, aber auch, um den Nutzer zu lokalisieren und ein Profil von ihm zu erstellen. Dieser Tracker wird also **Informationen über Sie sammeln** und Ihre Nutzung, genauso wie Cookies, nur eben auf Ihrem Smartphone.



Was sind Web-Beacons?

Web-Beacons werden von Unternehmen und Marketingfachleuten häufig verwendet, insbesondere in Newslettern und Werbe-E-Mails. Es handelt sich dabei um **einfache Bilder, die auf einem externen Server gehostet** und in Ihre E-Mails eingefügt werden. Sobald sie zur Anzeige in Ihren E-Mails hochgeladen werden, **sammeln und teilen diese Web-Beacons persönliche Informationen** wie das Datum und die Uhrzeit des Öffnens, den verwendeten Gerätetyp und das Betriebssystem oder Ihre IP-Adresse und geografische Position. Diese Informationen können dann gesammelt und verwendet werden, um ein Profil von Ihnen zu erstellen und Sie mit personalisierter Werbung anzusprechen. Einige dieser Tracker sind fast unsichtbar - sie erscheinen als kleine transparente Bilder, die nur dazu verwendet werden, zusätzliche Informationen über Sie zu sammeln.

Wie funktioniert Online-Werbung?

Werbung sehen wir jeden Tag: sei es in sozialen Netzwerken oder im Fernsehen, sei es, um uns Rabatte für unsere nächste Reise anzubieten oder für ein Produkt, das wir schon seit Wochen im Auge haben! Aber wissen Sie, wie das wirklich funktioniert?

An der Online-Werbung sind drei Akteure beteiligt:

- **Werbetreibende, die für ihr Produkt werben,**
- **die Werbeplattformen, auf denen die Werbung angezeigt wird,**
- **Tracking-Unternehmen, die eine ganze Reihe von Informationen sammeln über Sie.**

Wie wir in einem vorigen Absatz gesehen haben, hinterlässt jeder Nutzer Spuren im Internet. Diese Spuren können von Tracking-Unternehmen gesammelt werden, die die berühmten Werbe-Cookies auf unseren Computern und Smartphones ablegen, um Daten abzugreifen. Diese Daten können an Werbeplattformen weiterverkauft werden. Marken nutzen diese Plattformen dann, um für ihre Produkte zu werben. Die Rolle der Werbeplattformen wird darin bestehen, die Nutzer mit dem zu verkaufenden Produkt zu verbinden, indem sie ein Profil aus ihren persönlichen Surfdaten erstellen.

Ein Beispiel: Sie haben kürzlich nach einem tragbaren Lautsprecher gesucht.

Während Ihrer Suche hat das Tracking-Unternehmen Cookies auf Ihrem Gerät abgelegt. Es weiß also, dass Sie kürzlich nach diesem Produkt gesucht haben. Es wird diese Information an Werbeplattformen weiterverkaufen, die auf diese Weise Werbeflächen an Marken verkaufen, die Lautsprecher verkaufen. Wenn Sie sich also das nächste Mal einloggen, werden Ihnen Werbeanzeigen für tragbare Lautsprecher angezeigt.

Nicht sehr praktisch, wenn der Kauf persönlich ist oder wenn es sich um ein Geschenk handelt, oder?
Die GAFA (**Google, Apple, Facebook, Amazon**) sind die größten Werbeplattformen auf dem Markt.

Was ist ein Algorithmus?

Wenn man es schematisiert, ist ein Algorithmus eine Reihe von Operationen, mit denen ein Problem gelöst werden kann. Ein Kochrezept zum Beispiel ist sicherlich einer der einfachsten Algorithmen: Es handelt sich um eine Folge von Anweisungen, die zu einem Ergebnis führt. Es gibt natürlich auch komplexere.

Suchalgorithmen zum Beispiel: Sie sind eine Folge von Anweisungen, die aufgrund einer Suchanfrage ein Ergebnis liefern. Dieses Ergebnis kann ein Objekt in einem Bild, ein Wort in einem Text oder auch eine Liste von Webseiten sein.

Man kann sich einen Algorithmus ein wenig wie eine Produktionskette vorstellen: Man liefert Informationen als Input und erhält ein Ergebnis als Output.
So funktionieren übrigens auch die Suchmaschinen. Sie geben eine Suchanfrage ein und die Suchmaschine verwendet eine Reihe von Algorithmen, um alle Webseiten zu suchen, die Ihre Frage beantworten könnten.

Es gibt zwei Arten von Suchmaschinen:

Diejenigen, deren Suchergebnisse von Ihren persönlichen Informationen, Ihrem Geo-Standort, Ihrer Kultur und Ihrem Suchverlauf (gesuchte Rezepte, besuchte Nachrichten, Lieblingsseiten usw.) beeinflusst werden. Dies ist zum Beispiel bei Google der Fall.

Diejenigen, die diese Informationen nicht verwenden, weil sie keine persönlichen Daten sammeln, wie z. B. Qwant.
Die vorgeschlagenen Ergebnisse sind daher unparteiisch in dem Sinne, dass sie für alle gleich sind, unabhängig von Ihrem Profil.

Einige Algorithmen sind so konzipiert, dass sich ihr Verhalten im Laufe der Zeit ändert, je nachdem, welche Daten ihnen zur Verfügung gestellt wurden. Diese "selbstlernenden" Algorithmen fallen in den Forschungsbereich der Expertensysteme und der künstlichen Intelligenz. Sie werden in immer mehr Bereichen eingesetzt, von der Vorhersage des Straßenverkehrs bis hin zur Analyse von medizinischen Bildern.

Was ist eine Filterblase?

holidays

Eine Filterblase ist ein Konzept, bei dem **Algorithmen die Meinungen der Nutzer verzerren, indem sie Inhalte auf der Grundlage der Nutzerpräferenzen empfehlen**. Die Vorlieben der Nutzer sind durch Cookies bekannt, die von den Webseiten beim Surfen im Internet abgelegt werden.

Die Inhalte, die Ihnen dann im Laufe Ihrer Suche vorgeschlagen werden, sind überpersönlich und können eine Art Eingrenzung erzeugen, eine Isolierung in einer intellektuellen und informationellen Blase, die man als Filterblase bezeichnet.

Konkret können einige Suchmaschinen zwei Nutzern, die **die gleiche Suchanfrage stellen, unterschiedliche Ergebnisse anzeigen**.

Beispielsweise kann eine Suche nach einer Ferienunterkunft je nach Such- und Browserverlauf Ergebnisse für 5-Sterne-Hotels statt für Campingplätze oder Bed & Breakfasts liefern. Das gilt auch für die Nachrichten, die Ihnen angeboten werden, oder die Preise, die angekündigt werden. Ihre Lesegewohnheiten bringen Sie in bestimmte Schubladen, die Ihr Profil definieren. Die Nachrichten, die Ihnen vorgeschlagen werden, werden dann mit diesem Profil in Verbindung gebracht, wodurch Ihr kritischer Sinn eingeschränkt wird. Der Internetnutzer wird so **in einer Filterblase eingeschlossen**.

Die einzige Möglichkeit, nicht in dieser Blase gefangen zu sein, besteht darin, die Spuren, die Sie im Internet hinterlassen, so weit wie möglich zu begrenzen und die Sammlung Ihrer digitalen persönlichen Daten so weit wie möglich einzuschränken.

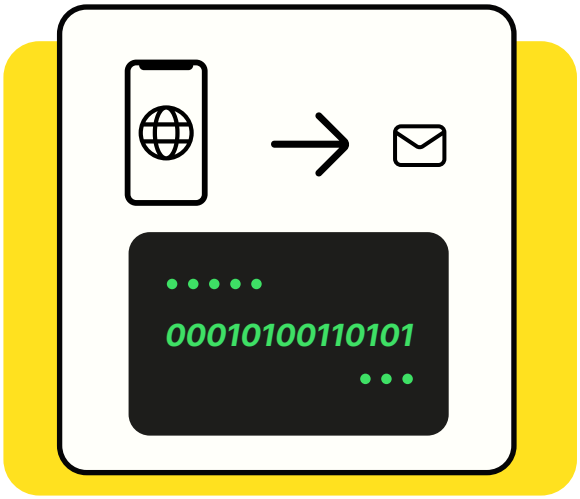
Was ist Verschlüsselung? Was ist mit End-to-End-Verschlüsselung?

Wenn Sie über das Internet kommunizieren, legen Ihre Daten potenziell Hunderte oder sogar Tausende von Kilometern zurück, bevor sie ihr Ziel erreichen. Kabel, Router und Server sind notwendig, um Ihre Daten zu transportieren. Bedeutet das aber, dass all diese Elemente zwangsläufig Zugriff auf alles haben, was Sie senden, obwohl sie nicht die endgültigen Empfänger sind? Nein, es ist möglich, Ihre Daten mithilfe der **Kryptografie**, der Wissenschaft von Geheimcodes, vor neugierigen Ohren zu schützen, und zwar durch einen Prozess, der als **"Verschlüsselung"** bezeichnet wird.

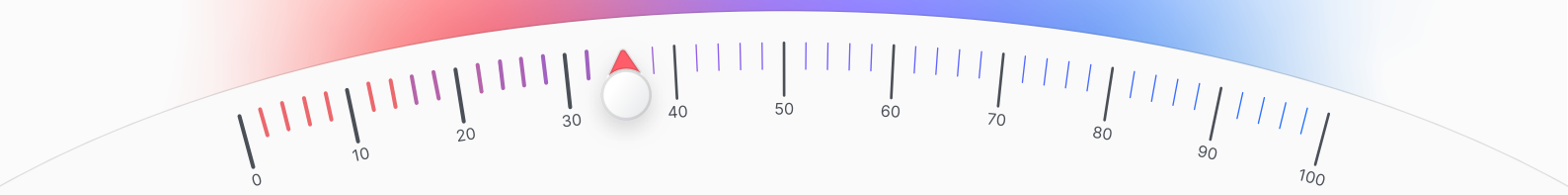
Nehmen wir ein Beispiel: Wenn Sie sich auf *https://www.qwant.com/* einloggen und dort eine Suche durchführen, wird Ihre Anfrage von Ihrem Browser automatisch "verschlüsselt", bevor sie an die Server von Qwant gesendet wird, wo sie "entschlüsselt" wird, sodass Qwant eine Liste mit relevanten Webseiten erstellen kann, die an Sie weitergeleitet werden können. Natürlich wird auch diese Liste von Qwant verschlüsselt, bevor sie an Sie gesendet wird. Ihr Browser entschlüsselt dann das Ergebnis, bevor er es Ihnen anzeigt. Das war's! Durch die Verschlüsselung sind Ihre Suchanfragen nur Ihnen und Qwant bekannt, die nicht wissen, wer hinter der Suche steckt.

Wir haben gesehen, wie Verschlüsselung Ihre Kommunikation mit einem Server, der einen Dienst anbietet, wie z. B. Qwant, sichert. Aber wie sieht es mit der Kommunikation zwischen Ihnen und einem anderen physischen Gesprächspartner aus? Hier kommt die "**End-to-End-Verschlüsselung**" ins Spiel.

Wenn Sie eine Nachricht über einen herkömmlichen Messenger an eine andere Person senden, wird sie in der Regel zwischen Ihrem Gerät (Smartphone oder Computer) und dem Server des Betreibers des Messenger-Dienstes verschlüsselt, der sie entschlüsselt und "unverschlüsselt" speichert, bis der Empfänger sie abholt. Die Nachricht wird dann zwischen dem Server und dem Endempfänger verschlüsselt. Dies wird als "**Punkt-zu-Punkt-Verschlüsselung**" bezeichnet. Was ist das Problem? Es ist, dass der Anbieter des Dienstes Zugriff auf alles hat, was Sie kommunizieren, obwohl er nicht der Endempfänger ist. Glücklicherweise gibt es eine Lösung: die sogenannte **End-to-End-Verschlüsselung**. Diese Technologie **stellt sicher, dass Ihre Nachrichten auf Ihrem Gerät verschlüsselt werden, bevor sie es verlassen, und nur an einem Ort entschlüsselt werden:** auf dem Gerät des Empfängers. Dazwischen bleiben Ihre Nachrichten verschlüsselt, auch wenn sie auf dem Server des Dienstanbieters gespeichert sind. Der Trick wird wieder gespielt!



Leider bieten nur wenige E-Mail-Dienste standardmäßig eine End-to-End-Verschlüsselung an. Dies ist zum Beispiel bei Gmail (für E-Mails) oder Telegram (für Instant Messaging) nicht der Fall. Das mag überraschend klingen: Letztendlich reproduziert die End-to-End-Verschlüsselung **in einer digitalen Welt nur das, was wir seit Jahrhunderten mit unseren physischen Briefen tun:** Wir stecken sie in Umschläge, bevor wir sie verschicken!



Die richtigen Reflexe, um Ihre Daten zu kontrollieren

" Heute ist es soweit! Ich kontrolliere die Spuren, die ich beim Surfen im Internet hinterlasse" Sie wissen nicht, wo Sie anfangen sollen? Wir helfen Ihnen! Erster Schritt: Frühjahrsputz. Nachdem alles gesäubert ist, rüsten wir uns aus.
3, 2, 1 ... los geht's!

2 Aufräumen

Löschen Sie Cookies und Ihren Browserverlauf.

Cookies zeichnen Ihre Aktionen, also Ihr Surfen im Internet, auf. Das erste, was Sie tun sollten, ist also aufräumen und **Ihre Cookies löschen.**

Wie gehen Sie dabei vor? Das hängt von Ihrem Browser ab!

Wenn Sie Firefox verwenden:

1. Klicken Sie in der Menüleiste am oberen oder unteren Bildschirmrand, je nach Gerät, auf Firefox und wählen Sie Einstellungen.
2. Wählen Sie den Datenschutz- und Sicherheitsbereich und gehen Sie zum Abschnitt Cookies und Websitedaten.
3. Klicken Sie auf die Schaltfläche Daten löschen und das gleichnamige Fenster erscheint.

   Die Kästchen für Cookies und Websitedaten (zum Löschen von Websiteverbindungen und Websiteeinstellungen) und Webinhalte im Cache (zum Löschen von Bildern, Skripten und anderen Webinhalten im Cache) sollten angekreuzt sein.
4. *Klicken Sie auf Löschen.*

Wenn Sie Safari verwenden:

1. IWählen Sie in der Safari-App auf Ihrem Mac Safari, dann Einstellungen und klicken Sie auf Datenschutz.
2. Klicken Sie auf Webseitendaten verwalten.
3. Wählen Sie eine oder mehrere Websites aus und klicken Sie dann auf Löschen oder Alle löschen.

Auf dem iPhone, um Ihre Cookies zu löschen, aber Ihren Verlauf beizubehalten,,

1. Gehen Sie zu Einstellungen > Safari > Erweitert > Websitedaten,
2. Klicken Sie auf Websitedaten löschen.

Wenn Sie Chrome verwenden:

1. Öffnen Sie auf Ihrem Computer Chrome.
2. Klicken Sie oben rechts auf Mehr bei den Einstellungen.
3. Klicken Sie auf Datenschutz und Sicherheit und dann auf Cookies und andere Websitedaten.
4. Klicken Sie auf Alle Daten und Berechtigungen von Websites anzeigen und dann auf Alle Daten löschen.
   Zur Bestätigung klicken Sie auf Löschen.

Überprüfen Sie Ihre Geolokalisierungseinstellungen

Nicht alle Apps müssen Ihre Bewegungen verfolgen, um zu funktionieren. Ein kurzer Blick in die Standorteinstellungen ist daher notwendig, um sicherzustellen, dass Ihre Einstellungen Ihren Wünschen entsprechen und nicht routinemäßig von allen Anwendungen, die Sie um Erlaubnis gefragt haben, vorgenommen werden.

Gehen Sie dazu wie folgt vor:

Auf Android :

1. Anwendungen
2. App-Berechtigung
3. Standort

Auf dem iPhone :

1. Einstellungen
2. Datenschutz
3. Ortungsdienste

Jetzt sind Sie dran: Entscheiden Sie, für welche Apps Sie die Ortung zulassen und für welche nicht!

Soziale Netzwerke aufräumen

Sind Sie nicht mit allen Fotos von Ihnen einverstanden? Möchten Sie den Zugang zu ihnen einschränken? Dann ist es an der Zeit, zu überprüfen, was man in sozialen Netzwerken über Sie wissen oder sehen kann.

Auf Instagram, TikTok und Facebook :

↪ **Schritt 1 :** Stellen Sie Ihr Konto auf privat um, wenn es das nicht schon ist.

↪ **Schritt 2 :** Sortieren Sie die Personen, die Ihr Konto abonniert haben, aus. Alte Bekannte, unbekannte Personen - es ist an der Zeit, die Personen zu sortieren, mit denen Sie Ihre Inhalte teilen möchten.

↪ **Schritt 3 :** Ihr Konto wurde vor einigen Jahren eingerichtet? Dann ist es vielleicht an der Zeit, einen Blick auf Ihre alten Beiträge zu werfen und zu überprüfen, ob Sie sich noch wohl dabei fühlen, all diese Fotos zu teilen.

↪ **Schritt 4 :** Überlegen Sie, bevor Sie Inhalte posten und bevor Sie eine Abonnementanfrage annehmen.

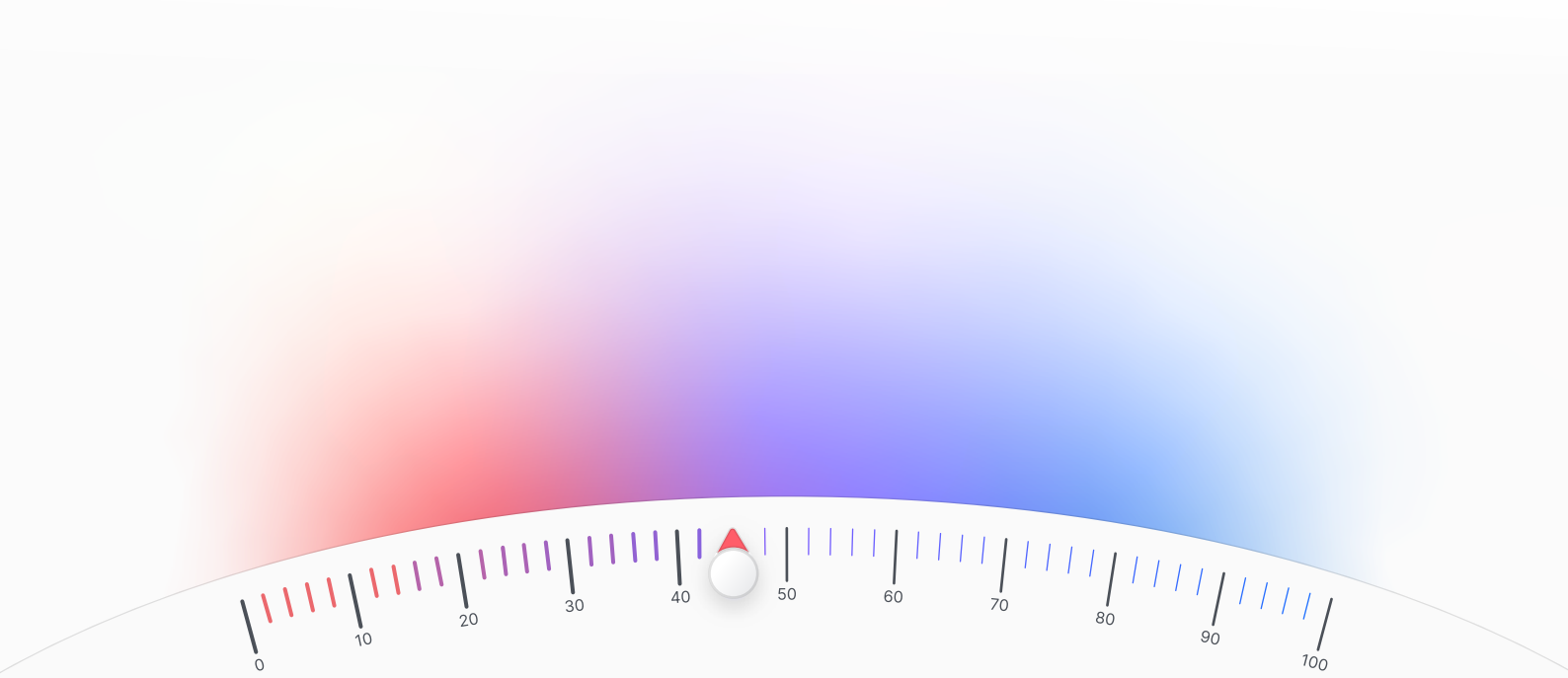
Überwachen Sie Ihre E-Reputation und machen Sie Ihr Recht auf Vergessen geltend.

Veröffentlichungen von Freunden, Namen, die mit Arbeiten, Veranstaltungen, sportlichen Leistungen oder früheren Aktivitäten in Verbindung gebracht werden... **aber was weiß das Internet über Sie?**
Um das herauszufinden, müssen Sie nur regelmäßig in eine beliebige Suchmaschine Ihren Vor- und Nachnamen, Ihre E-Mail-Adresse oder andere Daten eingeben, die Sie online mit anderen teilen und anhand derer Sie identifiziert werden können.

Was tun, wenn unerwünschte Inhalte veröffentlicht werden im Internet ?

Wenn es möglich ist und es sich nicht um eine böswillige Person handelt, können Sie direkt bei der Person, die die Veröffentlichung veranlasst hat, die Löschung beantragen.
Wenn dies nicht möglich ist oder Sie mit der Antwort nicht zufrieden sind, können Sie Ihr Recht auf Vergessenwerden geltend machen. **Die Datenschutzverordnung (DSGVO)** ermöglicht es jeder Person, die Löschung der sie betreffenden Daten zu verlangen. Dazu müssen Sie sich direkt mit der Website, von der die Veröffentlichung stammt, in Verbindung setzen und die URL, die zu löschenden Informationen und den Grund für Ihren Antrag angeben. Diese Inhalte können dann entfernt werden.

Gleichzeitig können Sie Suchmaschinen bitten, Inhalte, die Ihrem Namen schaden könnten, nicht mehr zu verknüpfen.



3 Sich ausrüsten, sich schützen

Jetzt, da die Hausarbeit erledigt ist, sind hier einige Verhaltensweisen, die Sie annehmen können.

Aktivieren Sie die Lokalisierung nur, wenn die Nutzung des Dienstes dies erfordert.

Nicht jede Anwendung, jede Website, die Sie besuchen, muss Ihre Bewegungen verfolgen und Ihren Standort jederzeit kennen. Nehmen Sie sich Zeit für die Entscheidung, wenn der Dienst den Zugriff verlangt: Warum muss diese Website meine Bewegungen verfolgen? Ermöglicht es mir, meinen Standort selbst einzugeben, um ein zufriedenstellendes Nutzererlebnis zu haben?
Passen Sie Ihre Antworten entsprechend an!

Verwenden Sie einen Browser und eine Suchmaschine, die respektvoller mit Ihren persönlichen Daten umgehen.

Ihr Tor zum Internet geht über einen Browser und eine Suchmaschine. Sie müssen also Ihre Gewohnheiten von Beginn der Erfahrung an ändern.
Wählen Sie dazu einen Browser und eine Suchmaschine, die respektvoller mit Ihren persönlichen Daten umgehen. Das gilt für Firefox als Browser oder auch für Brave oder die Qwant-App.

Testen Sie für Suchmaschinen Qwant (französische Suchmaschine) oder DuckDuckGo, Suchmaschinen, die Ihre persönlichen Daten nicht sammeln und daher nicht damit handeln.

Verwenden Sie privates Surfen

Das private Surfen ist eine in Browsern verfügbare Funktion, die es Ihnen ermöglicht, zu surfen, ohne dass Browserdaten wie Verlauf oder Cookies gespeichert werden auf Ihrem Gerät.

Beim privaten Surfen werden nach dem Beenden Ihrer Sitzung weder Ihr Browserverlauf noch Ihre Cookies gespeichert. Achtung: Dies hindert die Websites nicht daran, Cookies auf Ihrem Gerät abzulegen. Es handelt sich also um einen ersten Schritt, bevor Sie zu einem Tracking-Blocker wechseln.

Um im privaten Modus zu surfen, gehen Sie einfach zu Ihren Browsereinstellungen und öffnen Sie ein „neues privates Browserfenster“.

Lehnen Sie nicht notwendige Cookies ab

Wenn Sie keinen Cookie-Blocker haben, werden Sie von den meisten Webseiten aufgefordert, Cookies zu akzeptieren oder abzulehnen. Versuchen Sie, sie konsequent abzulehnen, oder akzeptieren Sie nur die Cookies, die für die Nutzung des Dienstes unerlässlich sind.

Dies ist jedoch umständlich, weshalb wir Ihnen den nächsten Schritt “Tracker-Blocker installieren“ vorschlagen.

Einen Tracking-Blocker installieren

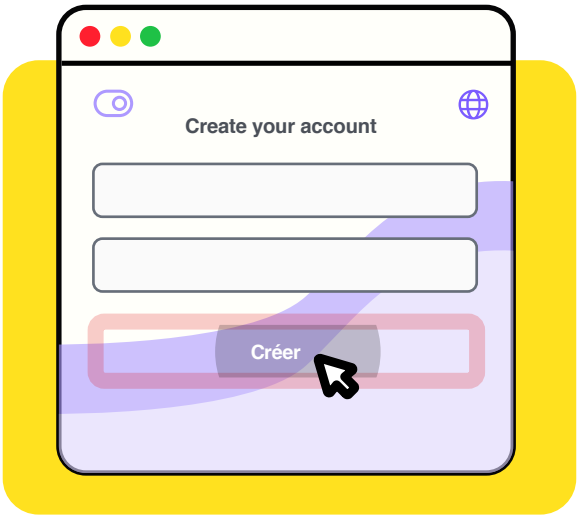
Um geschützt zu surfen, empfehlen wir Ihnen, **einen Cookie- und Tracking-Blocker zu installieren**. Dieser Blocker wird es Ihnen ermöglichen, vertraulich im Internet zu surfen.

Wir empfehlen Ihnen, die Browsererweiterung **Qwant VIPrivacy** zu installieren, die Cookies und Tracker beim Surfen blockiert und Qwant als Standardsuchmaschine installiert. Sie können auch **ein Tool zum Schutz vor Trackern verwenden oder einen E-Mail-Dienst nutzen, der Tracker automatisch blockiert**. Der verbesserte Tracking-Schutz von **Proton Mail** ist standardmäßig für alle Nutzer im Web und in der Proton Mail-App für iPhone und iPad aktiviert. Diese Funktion schützt Ihre Privatsphäre vor Tracking-Versuchen in Ihren E-Mails und gibt Ihnen mehr Ruhe. Sicheres und vertrauliches Surfen, von einem Ende Ihrer Suche bis zum anderen!

Wählen Sie Ihre E-Mail und Ihren Instant Messenger aus

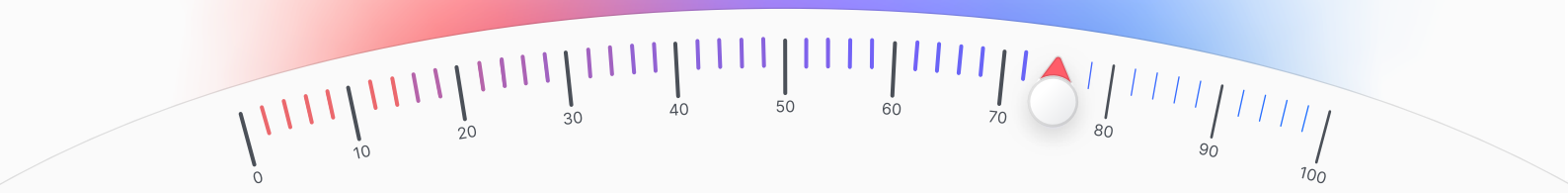
Um Ihre E-Mails, Ihren Kalender oder auch Ihr Drive zu sichern, empfehlen wir Ihnen, ein Konto auf der **Proton**-Website einzurichten.

Für Ihren Instant Messenger empfehlen wir Ihnen die Installation von **Olvid**, dem ersten privaten Messenger für alle, der kostenlos auf iOS und Android verfügbar ist.



In beiden Fällen steht der Schutz Ihrer persönlichen Daten an erster Stelle. Bei Olvid und Proton zum Beispiel müssen Sie dem Herausgeber nicht einmal eine Telefonnummer, eine Adresse oder einen Namen mitteilen... Im Fall von Olvid gibt es nicht einmal ein "Konto" auf einem Server irgendwo auf der Welt. Ganz einfach, weil Olvid **keine persönlichen Daten benötigt**, um zu funktionieren! Ihre Daten (wie z. B. Ihr Name) werden nur mit den Olvid-Nutzern geteilt, die Sie beschließen, einzuladen. Das Ergebnis: Olvid ist der einzige Messenger, der Ihnen garantieren kann, dass Sie niemals Spam erhalten.

Die Nutzung von E-Mail-Diensten, die per Design garantieren, dass sie keinen Zugriff auf Ihre persönlichen Daten haben, ist der einzige Weg, um sicherzugehen, dass ein Dienst, der sich als kostenlos anpreist, auch wirklich kostenlos ist. Solche Dienste gibt es. Warum sollten Sie auf sie verzichten?

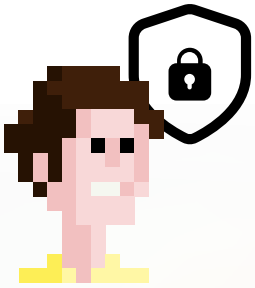


Verwenden Sie ein VPN

Ein **VPN (Virtual Private Network)** ist eine Software, die auf Geräten mit Internetanschluss installiert wird und **einen sicheren Tunnel zwischen Ihnen als Nutzer und dem Internet** herstellt.

Wenn Sie eine Verbindung zu einem VPN herstellen, wird Ihr gesamter Internetverkehr über den VPN-Server umgeleitet, bevor er auf der endgültigen Website ankommt. Die Verbindung mit einem VPN-Server wird dazu führen, dass Ihre IP-Adresse verborgen und auf die des Servers geändert wird. Letztendlich tritt der VPN-Server als Vermittler auf. So wird Ihre ursprüngliche IP-Adresse nicht an die von Ihnen besuchte Website weitergegeben und Ihre Privatsphäre wird respektiert.

Hier sind einige vertrauenswürdige Produkte, die Sie problemlos auf Ihrem Computer oder Handy installieren können: **Proton VPN**, Express VPN, CyberGhost, Mozilla VPN und NordVPN.



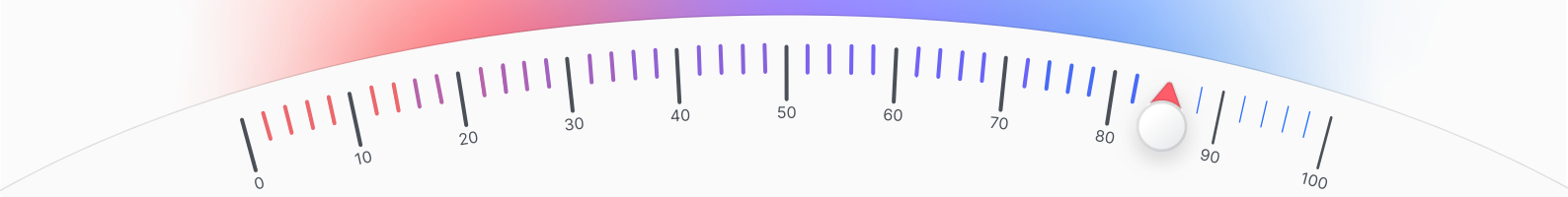
Sie haben nun alle Karten in der Hand, um Ihre Privatsphäre im Internet zu schützen: Jetzt liegt es an Ihnen!

Wählen Sie ein Smartphone, das Ihre persönlichen Daten nicht verwendet.

Es ist sehr wahrscheinlich, dass Ihr Smartphone Sie ohne Ihr Wissen ausspioniert. Die meisten herkömmlichen Smartphones sammeln eine riesige Menge an Daten von Ihrem Gerät, seien es Ihre Kontakte, Ihre Nutzung oder Ihre Bewegungen, und senden all diese Daten an Server bei Google, Apple, Facebook und anderen Tech-Giganten.

Die Murena-Smartphones wurden entwickelt, um Nutzern, die sich um ihre Privatsphäre sorgen und sich vor datenhungrigen Telefonen schützen möchten, einen anderen Ansatz zu bieten.
Sie basieren auf dem freien Betriebssystem "/e/OS", das vollständig "deGoogelt" ist: Standardmäßig sendet es keine Daten an Google und sammelt auch nicht Ihre Nutzungsdaten oder Ihren Standort.

Mit /e/OS kann man nicht nur einen "Privacy Score" für jede Android-Anwendung einsehen, bevor man sie installiert, sondern es ermöglicht auch, in Anwendungen versteckte Tracker zu blockieren und damit das Mikro-Targeting von Werbung zu unterbinden.



Diese Anleitung wurde Ihnen von Qwant, Proton, Olvid und Murena zur Verfügung gestellt; allesamt europäische Hauptakteure, die digitale Dienste anbieten, die die Privatsphäre ihrer Nutzer respektieren.

Qwant

Über **Qwant**

Developed in France and leader in Europe, Qwant ist die in Frankreich entwickelte und in Europa führende Suchmaschine, die die Privatsphäre ihrer Nutzer respektiert, indem sie keine persönlichen Daten sammelt.

Qwant entwickelt seine eigene Web-Indexierungstechnologie, die darauf ausgelegt ist, unvoreingenommene, umfassende und nicht profilierte Suchergebnisse zu liefern. So gewährleistet Qwant einen Internetsuchdienst mit null Suchtracking, null Werbetracking und null Verkauf von persönlichen Daten.

Neben den Diensten Qwant Search, Qwant Maps, einem Kartenangebot, und Qwant Junior, einer Suchmaschine für 6- bis 12-Jährige, bietet Qwant Qwant VIPrivacy an, eine Browsererweiterung, die es ermöglicht, das Web ohne Tracking-Werbung zu durchsuchen. Qwant ist im Web verfügbar: www.qwant.com, oder über Browsererweiterungen. Der Qwant-Browser ist für mobile iOS- und Android-Anwendungen verfügbar.Qwant hat 6 Millionen monatliche Nutzer.

Qwant weiß nichts über Sie, und das ändert alles!

www.qwant.com

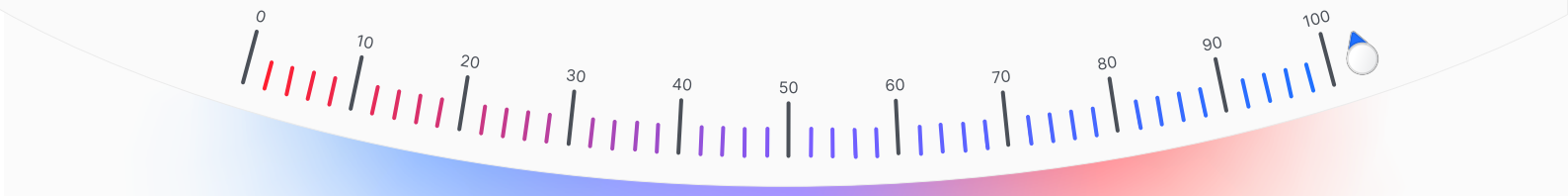
Proton

Über **Proton**

Das Unternehmen Proton wurde 2014 in der Schweiz von Wissenschaftlern gegründet, die sich bei der Europäischen Organisation für Kernforschung (CERN) kennengelernt haben. Unsere Vision ist es, ein Internet zu schaffen, in dem der Schutz der Privatsphäre die oberste Regel ist, und zwar durch ein Ökosystem von Diensten, die für jeden zugänglich sind, überall und zu jeder Zeit. Unser erstes Produkt, Proton Mail, ist mittlerweile der größte verschlüsselte E-Mail-Dienst der Welt. Die Nachfolgeprodukte Proton VPN, Proton Calendar und Proton Drive basieren auf derselben End-to-End-Verschlüsselung, die unseren Nutzern die volle Kontrolle darüber gibt, wie und mit wem ihre Daten geteilt werden.

Unsere Produkte sind Open Source, werden von einem 400-köpfigen Team entwickelt und von einer aktiven Community in über 180 Ländern unterstützt. Heute macht Proton den Schutz der Privatsphäre mit über 70 Millionen Benutzerkonten für alle zugänglich, von Journalisten über einige der größten Organisationen der Welt bis hin zu Einzelpersonen aus der ganzen Welt

https://proton.me/fr



Über Olvid

Olvid ist der erste private Instant Messenger für alle, der kostenlos für iOS und Android erhältlich ist.

Neben der systematischen End-to-End-Verschlüsselung all Ihrer Kommunikation garantiert Olvid auch eine End-to-End-Authentifizierung aller Gesprächspartner. Dies schützt Sie vor jeder Form von Spam und stellt sicher, dass nur die von Ihnen ausgewählten Nutzer sich mit Ihnen austauschen können. Da Olvid keine persönlichen Daten benötigt, um zu funktionieren (und somit auch keine von Ihnen verlangt), ist es grundsätzlich kostenlos.

Bilden Sie Gruppen mit Ihrer Familie, Ihren Verwandten und Ihren wichtigsten Mitarbeitern. Es ist nicht nötig, ein virtuelles Netzwerk von 5000 "Freunden" zu knüpfen. Olvid wurde entwickelt, um der beste Ort zu sein, um über die wichtigen Dinge zu sprechen, mit denen, die wichtig sind.

https://olvid.io

Über Murena

Gegründet 2018 von dem Open-Source-Veteranen Gaël Duval, Gründer von "Mandrake Linux", ist Murena ein Startup, das sich für den Schutz der Privatsphäre einsetzt mit transparenten und qualitativ hochwertigen Produkten und Dienstleistungen, die Bürgern helfen, der digitalen Überwachung zu entkommen.

Wir bei Murena sind davon überzeugt, dass Open-Source-Technologien der einzige Weg sind, dieses Versprechen einzulösen, da sie für maximale Transparenz vollständig überprüfbar bleiben. Murena entwirft /e/OS, ein mobiles Betriebssystem mit vorinstallierten Anwendungen, und Murena Cloud, eine Reihe von Online-Diensten, die /e/OS begleiten.

Murena entwickelt auch Murena-Telefone mit vorinstalliertem /e/OS, die heute erhältlich sind und in die USA, nach Kanada, Europa, Großbritannien und in die Schweiz geliefert werden.

https://murena.com

Contact : dataprivacyday@qwant.net