MICHAEL B. BARNES
BÜRGERANLIEGEN • STELLUNGNAHMEN • KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

24.07.2026

🛡️ HILFE! WER SCHÜTZT UNSERE KINDER UND UNS VOR DER POLITIK?

🛡️ Wenn „Kinderschutz“ als Trojanisches Pferd für die totale Internet-Kontrolle missbraucht wird

KAPITEL 1: VORWORT – WER SCHÜTZT UNS VOR DER POLITIK?

KAPITEL 1: VORWORT – WER SCHÜTZT UNS VOR DER POLITIK?

Wir müssen den Tatsachen ins Auge sehen: Es sind die Regierenden selbst, die den rechtschaffenen Bürgern das Leben im Internet durch immer neue Regulierungen und digitale Hürden systematisch unmöglich machen. Während die herrschende Politik unter dem Deckmantel des Schutzes eine lückenlose digitale Kontrolle hochzieht, zeigt sich ein unerträgliches und brandgefährliches Paradoxon im echten Leben.

Die journalistische Kernrecherche von Dominik Kettner

Um die immense Tragweite und Brisanz der folgenden Enthüllungen zu verstehen, müssen wir zuerst einen Blick darauf werfen, wer die Fakten ans Licht gebracht hat. Um sich nicht mit fremden Federn zu schmücken: Die journalistische Kernrecherche zu den Hintergründen der neuen EU-Altersverifikations-App stammt von Dominik Kettner, dem Gründer und Geschäftsführer des führenden Fachunternehmens Kettner Edelmetalle.

Um die immense Tragweite und Brisanz der folgenden Enthüllungen zu verstehen, müssen wir zuerst einen Blick darauf werfen, wer die Fakten ans Licht gebracht hat. Um sich nicht mit fremden Federn zu schmücken: Die journalistische Kernrecherche zu den Hintergründen der neuen EU-Altersverifikations-App stammt von Dominik Kettner, dem Gründer und Geschäftsführer des führenden Fachunternehmens Kettner Edelmetalle.

Kettner ist kein Unbekannter. Als ausgewiesener Finanz- und Wirtschaftsexperte landete er mit seinem aufrüttelnden Werk „Der digitale Euro – Die größte Enteignung der Geschichte“ auf Platz 1 der SPIEGEL-Bestsellerliste. Seine tiefe Skepsis gegenüber der zunehmenden Digitalisierung und dem Abbau von Bürgerrechten kommt nicht von ungefähr: Durch seine tägliche Arbeit mit physischen Sachwerten und Vermögenssicherung analysiert er seit Jahren die schleichenden Pläne der Zentralbanken und Regierungen zur Bargeldabschaffung und lückenlosen Bürgerüberwachung. Für seine tiefgründigen Analysen holt er regelmäßig hochkarätige Insider, Juristen und Ökonomen in sein Studio, um politische Nebelkerzen sachlich und rechtssicher zu demontieren. Was er in seinen Publikationen voraussagte, wird heute Schritt für Schritt bittere Realität.

Die unzensierten Fakten zur EU-Altersverifikation

Viele Bürger spüren es bereits im Alltag: Der Login bei Instagram, TikTok oder Facebook hakt, Konten sperren sich scheinbar grundlos. Während die Nutzer noch ratlos vor ihren Bildschirmen sitzen, tritt EU-Kommissionspräsidentin Ursula von der Leyen vor die Kameras und verkündet mit lächelndem Gesicht eine Nachricht, die tiefer blicken lässt als jedes gelekte Geheimdokument der Welt.

Ihre offizielle Botschaft lautet: „Unsere europäische App zur Altersverifikation ist technisch bereit und steht den Bürgern bald zur Verfügung. Diese App wird es den Nutzern ermöglichen, ihr Alter beim Zugriff auf Online-Plattformen nachzuweisen – genau wie Geschäfte nach einem Altersnachweis fragen, wenn Menschen alkoholische Getränke kaufen.“ Von der Leyen zieht in ihrer Rede selbst den direkten, entlarvenden Vergleich zur jüngsten Vergangenheit. Sie erinnert stolz daran, wie die Kommission während der Pandemie in einer Rekordzeit von nur drei Monaten die Covid-App entwickelte. Damals hieß es, das Scannen des Zertifikats sei ein „temporäres Notfallinstrument“. 78 Länder auf vier Kontinenten nutzten das System. Den offiziellen Beweis und die gesamte Erklärung zu dieser folgenschweren Technologie kannst du direkt im Presseportal der Europäischen Kommission nachlesen:
https://europa.eu

Und genau diesen „Erfolg“ überträgt die EU nun eins zu eins auf die Internet-Verifikation. Als Bestsellerautor Dominik Kettner diese Passage in seiner journalistischen Recherche einspielt und analysiert, wird das perfide Spiel aus Brüssel sofort offengelegt. Kettner kommentiert fassungslos: „Ich hatte Gänsehaut, als ich hörte, was hier gerade vorbereitet wird. Denselben

Prinzipien der Covid-Zeit, demselben Modell.“Die Enthüllungen von Dominik Kettner zeigen schonungslos, dass im Untergrund ein gigantischer, koordinierter Kontroll-Apparat hochgezogen wird. Die Behauptung, dass diese App dem Jugendschutz dient, bricht bei genauer Betrachtung der technologischen Fakten sofort in sich zusammen. Kettner legt offen, wer im Hintergrund die Fäden zieht und massiv an der Entrechtung der Bürger verdient.Die amtierende Politik hat den Bau dieser Infrastruktur klammheimlich an dieselben Großkonzerne übergeben, die bereits bei der Corona-Infrastruktur hunderte Millionen an Steuergeldern eingestrichen haben. SAP und die Deutsche Telekom bauen im Auftrag der Brüsseler Eliten ein zentralisiertes Netzwerk auf. Die Millionenbeträge und Verträge für diese Überwachungsinfrastruktur kannst du offiziell in den Berichten des Bundesrechnungshofes einsehen: https://www.bundesrechnungshof.deKettner warnt in seinen Analysen eindringlich vor den wahren Konsequenzen: Das System ist so aufgebaut, dass die Alters-App nahtlos mit der staatlich kontrollierten, digitalen Identität (Digital ID) verknüpft wird. Den unumstößlichen Beweis hierfür liefert das offizielle EU-Amtsblatt auf EUR-Lex, welches die gesetzliche Zusammenführung von Altersnachweisen und der europaweiten eIDAS-Identitätsinfrastruktur schwarz auf weiß dokumentiert: https://eur-lex.europa.eu
Es ist die totale Schikane und digitale Erpressung: Entweder du gibst deine intimste Privatsphäre an der staatlichen Schleuse ab, oder du fliegst komplett aus dem Internet. Kettner verknüpft dieses System mit den schleichenden Plänen zur Bargeldabschaffung und der Einführung des digitalen Euros. Das Ziel dieser elitären Gruppen im politischen Sumpf ist die absolute, unumstößliche Kontrolle über das Denken, das Schreiben und die Finanzen jedes einzelnen Bürgers. Damit kommt die unerträgliche Wahrheit im Untergrund ans Licht: Die Corona-App dient den Mächtigen heute als exakte technologische und psychologische Blaupause für eine dauerhafte, niemals endende Kontrolle des gesamten Internetzugangs. Es hat im Kern überhaupt nichts mit dem Schutz von Kindern zu tun! Der Kinderschutz wird von Brüssel nur als moralischer Vorwand missbraucht, um jede Gegenrede im Keim zu ersticken. Wer künftig das Netz nutzen will, muss sich über diese Infrastruktur digital vor dem Staat ausweisen. Und dass hier wieder dieselben Netzwerke verdienen, ist kein Zufall: Die Telekom und der Software-Riese SAP – die damals bereits über 214 Millionen Euro Steuergelder für die Corona-Warn-App kassierten – haben auch jetzt wieder den Auftrag erhalten, das System zu bauen. Mit dem Geld der Steuerzahler wird hier ein digitales Gefängnis hochgezogen.

Das ewige Muster der Mächtigen: Moral, Infrastruktur, Zwang

Wie Bestsellerautor Dominik Kettner lückenlos offenlegt, folgt der Weg in die totale digitale Kontrolle immer derselben dreistufigen Strategie:

1. Die moralische Erpressung: Am Anfang steht immer eine moralische Begründung, die so emotional aufgeladen ist, dass sie unangreifbar wirkt. Diesmal missbraucht man das Schutzbedürfnis unserer Kinder. Wer es wagt, die Überwachungsinfrastruktur kritisch zu hinterfragen, wird sofort gesellschaftlich mundtot gemacht und als „Gegner des Kinderschutzes“ gebrandmarkt.
2. Die schrittweise Gewöhnung: Die App wird als „innovative, nutzerfreundliche Lösung“ auf dem Silbertablett serviert. Sechs Länder haben das System bereits im Hintergrund getestet.
3. Der flächendeckende Zwang: Aus dem vermeintlich freiwilligen Werkzeug wird schleichend ein Standard, aus dem Standard eine absolute Voraussetzung. Am Ende betrifft es nicht mehr nur die Jugend, sondern jeden einzelnen Bürger, der sich im Internet bewegen möchte.

Das unerträgliche Paradoxon und der Kontrollverlust auf den Straßen

Betrachtet man diese Entwicklung aus der Vogelperspektive, stößt man auf eine unerträgliche und brandgefährliche Doppelmoral der herrschenden Politik, die die Bürger fassungslos zurücklässt: Während die Regierenden Abermillionen Fremde unkontrolliert ins Land lassen, wird der rechtschaffende, einheimische Bürger im digitalen Raum wie ein Schwerverbrecher unter Generalverdacht gestellt. Seit Beginn der Flüchtlingsbewegung unter der Merkel-Regierung sind bis heute über 4 Millionen Schutzsuchende nach Deutschland zugewandert. Allein im Jahr 2025 wurden 168.543 Asylanträge registriert, wobei der Anteil von im Inland geborenen Kleinstkindern unter den Antragstellern bei 15,6 Prozent lag.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Die bittere Realität, die vor der Regierungsbank verschwiegen wird, ist der vollständige Kontrollverlust auf unseren Straßen. Während die Politik die Grenzen offen ließ und die reale Sicherheit im Land kollabieren ließ, wodurch unzählige Menschen und insbesondere wehrlose Kinder im echten Leben Opfer von Gewalt wurden, dreht der Staat die Schuld um. Die Zahlen des Bundeskriminalamtes belegen dieses vollständige Versagen der Regierenden auf dramatische Weise. Während die Politik wegschaut, zeigt die offizielle Polizeiliche Kriminalstatistik des BKA, dass im Bereich der Gewaltkriminalität nichtdeutsche Tatverdächtige mit rund 43 Prozent massiv überrepräsentiert sind. Die polizeilichen Daten zeigen schwarz auf weiß: Die Kriminalitätsbelastung ist bei dieser Gruppe etwa viermal höher als bei der deutschen Bevölkerung. Besonders verwerflich ist, dass im Zuge dieser Entwicklung erwiesenermaßen immer mehr unschuldige Kinder im realen Leben zu Schaden kommen, was sich auch im kontinuierlichen Anstieg tatverdächtiger Kinder in den Kriminalstatistiken widerspiegelt.
Hier wird ein Schuh daraus: Die reale und akute Bedrohung für Leib und Leben geht von dem durch die Politik verursachten Kontrollverlust aus. Anstatt jedoch genau hier anzusetzen, die Grenzen rigoros zu sichern und das eigene Volk vor dieser Gewalt zu schützen, erlassen die Mächtigen lieber Gesetze zur digitalen Totalüberwachung. Sie stellen den rechtschaffenen Bürger unter Generalverdacht, während auf unseren Straßen das Chaos regiert. Das ist die absolute Bankrotterklärung einer Regierung, die die Augen vor den echten Opfern verschließt und stattdessen die Privatsphäre der eigenen Bevölkerung vernichtet.

Die Verantwortlichen im politischen Sumpf

Dieses historische Versagen und die aktuellen Zustände in unserem Land haben wir einzig und allein den etablierten Altparteien der amtierenden Politik zu verdanken. Weder die AfD noch das BSW tragen hierfür die Schuld, da sie sich nicht in der Regierungsverantwortung befinden. Das ständige, ermüdende Framing in den Medien gegenüber alternativen politischen Kräften dient nur als Ablenkungsmanöver, um von den echten, drastischen Problemen im Land abzulenken. Es gibt einflussreiche Gruppen in diesem politischen Sumpf, die diese Zustände und den Verlust unserer Privatsphäre ganz bewusst so wollen.
Dass es hierbei niemals um den echten Schutz von Kindern ging, beweist Kettner zudem mit einem Blick nach London. Ausgerechnet der britische Premierminister Keir Starmer inszeniert sich heute als der große Kinderschützer im Netz. Doch als Starmer von 2008 bis 2013 Chef der britischen Staatsanwaltschaft war, wurden im berüchtigten Rotherham-Skandal nachweislich mindestens 1.400 Kinder rituell und systematisch missbraucht. Die Behörden unter seiner Führung stuften die Hauptzeugin als „unglaubwürdig“ ein und stellten die Verfahren einfach ein. Echte Opfer, echte Täter, greifbare Akten – und die Justiz schaut weg. Wenn genau diese Politiker heute im Namen des „Kinderschutzes“ eine totale Internet-Überwachung fordern, ist das an Verlogenheit nicht zu übertreffen. Es geht ihnen nicht um den Schutz der Schwachen. Es geht um die lückenlose Kontrolle darüber, wer was im Internet liest, schreibt und denkt.

Deine Verteidigungslinie: Warum Abwarten keine Option mehr ist

Wenn die größte Gefahr für unsere Freiheit von staatlichen Gesetzen und digitalen Identitäts-Zwängen ausgeht, dürfen wir nicht länger passiv bleiben. Echte Sicherheit im Netz gibt es nicht geschenkt – wir müssen sie uns selbst von den Mächtigen zurückholen. Digitale Selbstverteidigung ist heute kein Hobby mehr für IT-Spezialisten, sondern Bürgerpflicht für jeden, der frei bleiben will.
Wer wegschaut, wird kontrolliert. Wer handelt, bleibt frei!
Dass es sich hierbei um keinen Brüsseler Alleingang, sondern um einen global koordinierten Plan elitärer Netzwerke handelt, beweist ein direkter Blick nach London und Australien. Fast zeitgleich preschte die australische Regierung mit Netzsperren voran. Und noch am selben Tag postete der britische Premierminister Keir Starmer auf der Plattform X, dass er „alles tun wird, was benötigt wird, um Kinder im Internet sicher zu machen“.
Hinter dieser weltweiten, zeitgleichen Kampagne im Namen des Kinderschutzes steckt jedoch bittere Heuchelei. Die historischen Fakten der britischen Justiz zeichnen ein völlig anderes Bild von den wahren Absichten dieser Akteure. Während Keir Starmers Amtszeit als Leiter der britischen Staatsanwaltschaft von 2008 bis 2013 ereignete sich der tiefgreifende

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Missbrauchsskandal von Rotherham, bei dem mindestens 1.400 Kinder rituell und systematisch missbraucht wurden.
Die Strafverfolgungsbehörden unter seiner Führung versagten damals auf ganzer Linie, stuften die Hauptzeugin als unglaubwürdig ein und stellten die Ermittlungen einfach ein. Echte Opfer, echte Täter, greifbare Akten – und keine Strafverfolgung. Die unzensierten, offiziellen Untersuchungsberichte zu diesem historischen Behördenversagen sind direkt im Regierungsportal des UK Government Home-Office für jeden unabhängig nachprüfbar dokumentiert:
www.gov.uk
Wenn genau diese elitären Kreise, die beim realen Schutz weggeschaut haben, nun zeitgleich eine lückenlose Internet-Überwachung fordern, ist das an Verlogenheit nicht zu übertreffen. Es geht ihnen nicht um den Schutz der Schwachen. Es geht um die lückenlose Kontrolle darüber, wer wann welche Seite im Internet aufruft, liest und denkt.

Deine Verteidigungslinie: Warum Abwarten keine Option mehr ist

Wenn die größte Gefahr für unsere Freiheit von staatlichen Gesetzen, Schikanen und digitalen Identitäts-Zwängen der Mächtigen ausgeht, dürfen wir nicht länger passiv bleiben. Echte Sicherheit im Netz gibt es von der herrschenden Politik nicht geschenkt – wir müssen sie uns selbst von den Entscheidungsträgern zurückholen. Digitale Selbstverteidigung ist heute kein Hobby mehr für IT-Spezialisten, sondern Bürgerpflicht für jeden, der frei bleiben will.
Wer wegschaut, wird kontrolliert. Wer handelt, bleibt frei!

KAPITEL 2: DAS E-MAIL-POSTFACH – DER GENERALSCHLÜSSEL ZU DEINEM LEBEN

Die reale Gefahr im Alltag: Das eigene E-Mail-Postfach ist der absolute Mittelpunkt unseres gesamten digitalen Daseins. Ob Online-Banking, Amazon, soziale Netzwerke wie Facebook und X oder staatliche Zugänge: Fast jede Registrierung im Internet läuft über deine E-Mail-Adresse.

Das macht dein Postfach zum begehrtesten Ziel für Kriminelle. Wenn Hacker Zugriff auf deine E-Mails erlangen, können sie bei all deinen anderen Konten einfach auf „Passwort vergessen“ klicken. Sie erhalten den Bestätigungslink direkt in dein geknacktes Postfach und übernehmen im Handumdrehen dein gesamtes Leben.

Viele Menschen wiegen sich in Sicherheit, weil sie seit Jahrzehnten bei großen Traditionsanbietern sind. Doch die Realität sieht anders aus: Erst kürzlich wurde wieder über massive Datenlecks berichtet, bei denen sensible Kundendaten im Darknet gelandet sind. Regelmäßig tauchen Berichte über gestohlene Passwörter auf, die zeigen, wie massiv Nutzerdaten durch Schadsoftware im Alltag abgegriffen werden. Während der Staat den unbescholtenen Bürger mit der Chatkontrolle bis ins intimste Detail ausspionieren will, schaut er bei den echten Datenkraken und den Sicherheitslücken der Großkonzerne weg. Wer auf Nummer sicher gehen will, lässt seine Konten von Zeit zu Zeit überprüfen. Professionelle Sicherheitssoftware meldet unbefugte Datenabflüsse sofort. Die offizielle Webseite von Kaspersky zur Überprüfung findest du hier: kaspersky.de Ob deine eigene E-Mail-Adresse bereits in kriminellen Datenbanken im Netz kursiert, lässt sich zudem über den kostenlosen Identity Leak Checker des Hasso-Plattner-Instituts sekundenschnell überprüfen. Die direkte Prüfseite lautet:hpi.deDen vollständigen und ausführlichen Leitfaden zu diesem Thema findest du in unserem Dokument Nummer 84: www.klartext-info.online oder https://www.klartext-info.online/digitale-selbstverteidigung-im-internet/

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Die Datenskandale der großen Provider

Viele Menschen wiegen sich in Sicherheit, weil sie seit Jahrzehnten bei großen Traditionsanbietern sind. Doch die Realität sieht anders aus: Erst kürzlich wurde wieder über massive Datenlecks berichtet, bei denen sensible Kundendaten im Darknet gelandet sind. Regelmäßig tauchen Berichte über gestohlene Passwörter auf, die zeigen, wie massiv Nutzerdaten durch Schadsoftware im Alltag abgegriffen werden.

Wer auf Nummer sicher gehen will, lässt seine Konten von Zeit zu Zeit überprüfen. Professionelle Sicherheitssoftware meldet unbefugte Datenabflüsse sofort.

Link: kaspersky.de

Ob deine eigene E-Mail-Adresse bereits in kriminellen Datenbanken im Netz kursiert, lässt sich zudem über den kostenlosen Identity Leak Checker des Hasso-Plattner-Instituts sekundenschnell überprüfen.

Link: hpi.de

Die goldene Regel gegen Phishing: Der Blick in die App

Hacker versuchen täglich, über gefälschte Rechnungen oder dringende Zahlungsaufforderungen per Mail an deine Daten zu kommen. Doch ein geschulter Blick entlarvt diese Betrüger: Die Formatierung ist fehlerhaft oder weicht vom Original ab. Die wichtigste Praxis-Regel lautet hier: Ignorieren und niemals Links in solchen E-Mails öffnen!

Wenn ein Anbieter, eine Bank oder eine Plattform wirklich etwas Wichtiges von dir will, hinterlässt er diese Nachricht grundsätzlich direkt in deinem persönlichen Account oder in der offiziellen Smartphone-App – und nicht im ungeschützten Postfach. Gehe im Zweifelsfall immer manuell über die offizielle Webseite oder die App des Anbieters, um den Status zu prüfen. Rechnungen von echten Bestellungen erkennst du daran, dass sie fehlerfrei geschrieben sind und dich korrekt mit deinem vollständigen Namen ansprechen.

Digitale Selbstverteidigung mit Sinn und Verstand

Der beste Schutz vor Cyber-Kriminellen ist ein gesundes Misstrauen. Wenn du eine Nachricht oder einen Absender – insbesondere aus dem Ausland – nicht zweifelsfrei einordnen kannst, lass im Zweifelsfall einfach die Finger davon. Wer als Anfänger kopflos agiert, verliert. Wer mit Sinn und Verstand vorgeht, bleibt sicher.

Die absolute Basislinie für ein unknackbares System besteht aus zwei simplen, aber hochwirksamen Schutzmauern: Zufällig generierte, starke Passwörter, die man sich niemals im Kopf merken kann, sowie die Aktivierung der Zwei-Faktor-Authentisierung (2FA). Das Bundesamt für Sicherheit in der Informationstechnik betont in seinen Leitfäden, dass diese Kombination die wichtigste Hürde gegen Identitätsdiebstahl ist.

Link: bund.de

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

KAPITEL 3: DIE ZWEI-FAKTOR-AUTHENTISIERUNG – DAS UNKNACKBARE SCHUTZSCHILD

Bisher schützten die meisten Menschen ihre Konten nur mit einem einfachen Passwort. Wenn dieses Passwort jedoch bei einem Datenskandal gestohlen wird, ist das Konto sofort offen. Die Zwei-Faktor-Authentisierung schließt diese Sicherheitslücke komplett. Sie funktioniert wie ein Tresor mit zwei verschiedenen Schlössern: Um dich anzumelden, brauchst du nicht mehr nur dein Passwort, sondern zusätzlich einen zweiten, kurzzeitigen Bestätigungscode, den du direkt auf dein eigenes Smartphone geschickt bekommst.

Warum Hacker hier absolut chancenlos sind

Selbst wenn ein hochprofessioneller Hacker dein Passwort erbeutet hat, kann er sich ohne diesen zweiten Code von deinem Smartphone nicht einloggen. Er steht vor einer verschlossenen Tür. Die amtierende Politik drängt uns in eine totale Abhängigkeit von staatlich kontrollierten Identitäts-Apps. Das BSI betont in seinen Empfehlungen zum Accountschutz jedoch, dass wir diese echten Schutzmaßnahmen selbst in die Hand nehmen müssen, anstatt den Kontroll-Systemen der Machthaber zu vertrauen. Man muss sich lediglich einmal die Mühe machen, diese Funktion in den Einstellungen des eigenen Mail-Anbieters einzuschalten, um seine digitale Festung gegen den staatlichen und kriminellen Zugriff zu sichern.

Die offizielle Informationsseite des BSI erreichst du unter:
bund.de

Wie dieses Prinzip der zwei Faktoren genau funktioniert und warum es jeden Login bombensicher macht, zeigt das verbraucherfreundliche Erklärvideo zur Zwei-Faktor-Authentisierung direkt beim BSI-Verbraucherportal:
bund.de

ENDE VON KAPITEL 3

KAPITEL 4: PASSWORT-SICHERHEIT UND DIE FESTUNG DER VERSCHLÜSSELTEN ANBIETER

Das große Risiko einfacher Passwörter: Der häufigste Fehler im Internet ist die Bequemlichkeit bei Passwörtern. Viele Menschen nutzen extrem einfache Passwörter oder verwenden ein und dasselbe Kennwort für mehrere Seiten gleichzeitig. Wird dann nur ein einziger Anbieter gehackt, bricht dein gesamtes digitales Kartenhaus zusammen. Ein sicheres Passwort muss lang sein, aus einer wirren Kombination von Zeichen bestehen und darf niemals ungeschützt im Browser gespeichert werden.

Die sichere Alternative zu den alten Anbietern

Wer den traditionellen Großanbietern nach den vielen Datenskandalen und der offensichtlichen Zusammenarbeit mit Behörden nicht mehr vertrauen möchte, findet heute extrem sichere Alternativen. Ein hervorragendes Beispiel ist der Anbieter Proton Mail, der seinen expliziten Sitz in

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

der Schweiz außerhalb der direkten EU-Zensurgewalt hat und einen komplett kostenlosen, werbefreien Grundzugang anbietet.

Der riesige Vorteil wird in den offiziellen Sicherheitsfunktionen von Proton-Mail erklärt: Durch eine sogenannte Null-Zugriff-Verschlüsselung sind deine E-Mails so stark geschützt, dass nicht einmal der Anbieter selbst oder Behörden deine Nachrichten mitlesen können. Kombiniert mit einem starken Passwort und der Zwei-Faktor-Authentisierung wird dein Postfach damit für Angreifer und staatliche Überwachungssysteme so gut wie unangreifbar. Es ist der direkte Mittelfinger gegen die Brüsseler Schikane. Die offizielle Seite von Proton Mail erreichst du unter:
https://proton.me

ENDE VON KAPITEL 4

KAPITEL 5: ANONYM SURFEN – VPNS UND DATENSCHUTZFREUNDLICHE BROWSER

Die Tarnkappe für deine Internetleitung (VPN): Wenn du dich ganz normal im Internet bewegst, hinterlässt du bei jedem Klick Spuren. Dein Internetanbieter und jede besuchte Webseite kennen deine genaue IP-Adresse und können dein Surfverhalten lückenlos protokollieren. Ein virtuelles privates Netzwerk, kurz VPN, funktioniert hier wie ein digitaler Tunnel. Das Bundesamt für Sicherheit in der Informationstechnik erklärt die Funktionsweise eines VPN ausführlich: Die Daten zwischen deinem Endgerät und dem Server werden komplett verschlüsselt und sind für Außenstehende nicht mehr einsehbar.

Dass diese Technologie ein vollkommen legales Werkzeug zum Schutz der Privatsphäre ist, hat der Europäische Gerichtshof in einem Grundsatzurteil ausdrücklich bestätigt. Das offizielle Urteil zur Rechtmäßigkeit von VPNs kann in der Rechtsprechungs-Datenbank des EuGH eingesehen werden:
europa.eu

Alternative Browser statt Datenkraken

Die Standard-Browser auf unseren Geräten leiten massenhaft Daten über dein Nutzungsverhalten an die Großkonzerne weiter. Eine hervorragende, datenschutzfreundliche Alternative ist der quelloffene Brave Browser, der Tracker und Werbung von Haus aus blockiert. Wer die maximale Anonymität sucht, greift zum Tor Browser. Wie das BSI zum Thema Tor-Netzwerk ausführt, leitet dieser Browser deine Verbindung dreifach verschlüsselt über verschiedene Knotenpunkte um. Dadurch wird es für Werbenetzwerke und Überwachungssysteme so gut wie unmöglich, deine echte IP-Adresse oder deinen physischen Standort zurückzuverfolgen. Die offizielle BSI-Erklärung zum VPN-Schutz findest du hier:
bund.de

ENDE VON KAPITEL 5

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

KAPITEL 6: ANONYM SURFEN UND STAATLICHE VPN-SPERREN IM NOTFALL UMGEHEN

Der Ernstfall: Was tun, wenn VPNs plötzlich verboten oder blockiert werden? Sollte der Staat oder dein Provider versuchen, normale VPN-Verbindungen flächendeckend zu blockieren, bricht deine normale Schutzmauer ein. In so einem Fall von Netzzensur kannst du die Sperren mit ausländischer Sicherheitssoftware durch drei konkrete, praktische Handgriffe sofort umgehen:

Punkt 1 – „Verschleierte Server“ in der App aktivieren

Normale VPN-Verbindungen werden von Blockadesystemen sofort erkannt und abgeschaltet. Große ausländische Premium-Anbieter haben dafür eine eingebaute Tarnfunktion. Die Umsetzung: Öffne die Einstellungen deiner VPN-App und stelle das Protokoll auf OpenVPN um. Nun wird in der Serverliste der Punkt „Spezialserver“ sichtbar. Klicke dort auf verschleierte Server oder den „Camouflage Mode“ deines Anbieters. Diese Funktion verändert die Datenpakete so, dass sie für den Provider wie ganz normaler, harmloser Internetverkehr aussehen. Die staatliche Sperre greift ins Leere. Die genaue Funktionsweise dieser Technologie wird auf der offiziellen Hilfeseite von NordVPN detailliert erklärt: https://nordvpn.com

Punkt 2 – Das Protokoll manuell auf „TCP-Port 443“ umstellen

Sperren blockieren oft nur das standardmäßige Übertragungsprotokoll deines VPNs. Du kannst den Tunnel jedoch manuell umleiten. Die Umsetzung: Gehe in die erweiterten Verbindungseinstellungen deiner Sicherheitssoftware. Schalte dort das Protokoll von UDP auf TCP um und wähle als Ausgang den Port 443. Port 443 ist derselbe Kanal, über den das gesamte weltweite Online-Banking und alle sicheren HTTPS-Webseiten laufen. Ein Provider kann diesen Port nicht sperren, ohne das gesamte wirtschaftliche Internet des Landes komplett lahmzulegen.

Punkt 3 – Den Tor-Browser mit „Bridges“ (digitalen Brücken) starten

Sollten kommerzielle VPN-Anbieter komplett verboten und deren Server-IPs blockiert werden, hilft nur noch das dezentrale, unzensierbare Tor-Netzwerk. Die Umsetzung: Lade dir den kostenlosen Tor Browser herunter. Wenn das normale Laden blockiert wird, klicke beim Starten auf „Konfigurieren“ und gehe zum Abschnitt „Brücken“. Klicke dort auf „Brücken anfordern“. Das System nutzt nun geheime, private Relays. Wie diese privaten Brücken-IPs funktionieren und warum sie von staatlichen Zensoren unmöglich flächendeckend blockiert werden können, erklärt die offizielle Dokumentation zur Zensurumgehung im Tor Project Support Portal:
torproject.org

ENDE VON KAPITEL 6

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

KAPITEL 7: DIE CHECKLISTE FÜR DEINE DIGITALE FREIHEIT

Deine tägliche Verteidigungslinie: Sicherheit im Internet ist kein Zustand, sondern ein fortlaufender Prozess. Nachdem wir die realen Mechanismen der Überwachung aufgedeckt und analysiert haben, liegt es an dir, aktiv zu bleiben. Nutze die folgende Checkliste, um deine Konten Schritt für Schritt in eine unknackbare digitale Festung zu verwandeln:

Die konkreten Schritte für den Alltag

• E-Mail-Postfach sichern: Aktiviere sofort die Zwei-Faktor-Authentisierung (2FA) bei deinem Provider oder wechsle zu einem komplett verschlüsselten Anbieter.
• WhatsApp-Backup verschlüsseln: Generiere den 64-stelligen Sicherheitsschlüssel in den Chat-Einstellungen. Schreibe den Code per Hand ab und lege ihn sicher in deine analoge Dokumentenmappe. Vertraue keinem Cloud-Backup.
• Datenspuren verwischen: Nutze im Alltag einen datenschutzfreundlichen Browser und ein verschlüsseltes VPN, um deine IP-Adresse vor den Augen der Mobilfunkriesen und Werbenetzwerke zu verbergen.
• Sperren im Ernstfall umgehen: Merk dir die Notfall-Schritte für dein VPN. Schalte bei Blockaden auf verschleierte Server (Camouflage Mode) um oder nutze den Tor-Browser mit privaten Brücken (Bridges).

Den Druck auf die Politik erhöhen und Rechte kennen

• Recht auf ein Konto kennen: Das sogenannte De-Banking darf dich nicht finanziell isolieren. Informiere dich unabhängig über das Recht auf ein Basiskonto, das jedem Bürger gesetzlich zusteht, direkt beim Bundesministerium der Justiz:
bmj.de
• Abgeordnete kontaktieren: Nutze dein Recht auf Gehör. Über die offizielle Abgeordnetensuche des Deutschen Bundestages kannst du deine regionalen Vertreter heraussuchen und deinen Unmut über die digitale Totalüberwachung sowie den Kontrollverlust auf den Straßen direkt an die politischen Gremien senden:
bundestag.de
• Wahlprogramme prüfen: Übernimm auch im echten Leben Verantwortung. Informiere dich unabhängig abseits der etablierten Medien und setze an der Wahlurne ein bewusstes Zeichen für Freiheit und Bürgerrechte.

ENDE VON KAPITEL 7

KAPITEL 8: DAS FAZIT – WARUM DIGITALE SELBSTVERTEIDIGUNG PFLICHT IST!

Die Digitalisierung hat uns viele Erleichterungen gebracht, aber sie hat uns auch so verletzlich gemacht wie nie zuvor. Wer heute die Augen verschließt und blind den Standardeinstellungen der

großen Tech-Konzerne, Mobilfunkriesen und politischen Vorgaben vertraut, gibt freiwillig den Schlüssel zu seiner eigenen Freiheit ab.

Hier sind die drei unumstößlichen Gründe, warum du das Schutzschild ab heute niemals mehr herunterfahren darfst:

1. Deine Privatsphäre ist dein Eigentum

Wenn du deine Daten nicht selbst aktiv schützt, macht der Staat dich durch Gesetze wie die geplante europäische Chatkontrolle vollkommen gläsern. Was einmal im Netz gelandet ist, kriegst du nie wieder zurück.

2. Der Schutz der Konzerne und der Politik ist eine Illusion

Die ständigen Skandale und massiven Datenlecks bei Traditionsanbietern zeigen, dass niemand deine Konten für dich sichert. Ein gehacktes Postfach ist der Generalschlüssel zu deinem gesamten Leben – die Riegel dafür musst du mit der Zwei-Faktor-Authentisierung selbst vorschieben. Während die herrschende Politik das Volk im realen Alltag auf den Straßen nicht mehr schützen kann, versucht sie im digitalen Raum die totale Ausspionierung. Wir haben über diese gefährlichen Entwicklungen und die drastischen Pläne der Politik bereits im Vorfeld ausführlich und detailliert berichtet. Den vollständigen, unzensierten Leitfaden zur Absicherung deiner Konten findest du unter: https://www.klartext-info.online/digitale-selbstverteidigung-im-internet/

3. Konsequente Vorsorge statt Schadensbegrenzung

Es ist viel einfacher und sicherer, die digitale Festung durch dauerhaft eingeschaltete VPNs und datenschutzfreundliche Browser von vornherein hochgezogen zu lassen. Mach es Angreifern, Datenkraken und staatlichen Überwachungssystemen im Alltag von der ersten Sekunde an systematisch so schwer wie möglich.

Nimm deine digitale Selbstbestimmung jetzt selbst in die Hand. Wer wegschaut, wird kontrolliert. Wer handelt, bleibt frei!

Mit freundlichen Grüßen

Michael B. Barnes

Michael B. Barnes

Impressum / Kontakt:
Michael B. Barnes
Hengeloer Str.1
49565 Bramsche
E-Mail: info@klartext-info.online

Rechtliche Hinweise & Urheberrecht:
Die Inhalte dieses Dokuments dienen ausschließlich der allgemeinen Information und Aufklärung. Sie stellen keine Rechts-, Steuer-, Finanz- oder Anlageberatung dar und können eine solche nicht ersetzen. Es wird keine Haftung oder Gewähr für die Richtigkeit, Aktualität und Vollständigkeit der Informationen übernommen. Die Nutzung erfolgt auf eigene Verantwortung. Alle Inhalte und Texte sind urheberrechtlich geschützt. Jede Vervielfältigung oder Verbreitung außerhalb der gesetzlichen Grenzen bedarf der vorherigen schriftlichen Zustimmung des Herausgebers.

Impressum:
https://www.klartext-info.online/impressum/

Zur Klartext-Info-Website

QR-Code

Weitere Beiträge, Aktualisierungen und Quellen:
www.klartext-info.online

Michael B. Barnes

Stand: 24.07.2026

ANHANG: PRAXIS-BEISPIEL FÜR DEINE DIGITALE SELBSTBESTIMMUNG

Wer handelt, bleibt frei! Um dir zu zeigen, wie du den Druck auf die Verantwortlichen im Alltag konkret erhöhst, findest du hier mein offizielles Kündigungs- und Beschwerdeschreiben an die Deutsche Telekom. Du kannst diesen Text als Vorlage nutzen, deine Daten einsetzen und ihn als klares Zeichen für deine Privatsphäre an deinen Anbieter senden:

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Betreff: Kundennummer [Deine Kundennummer] – Kündigung zum Ende der Mindestvertragslaufzeit und Mitteilung meiner Beweggründe

Sehr geehrte Damen und Herren,

ich habe erst vor Kurzem einen Vertrag mit Ihrem Unternehmen abgeschlossen. Nach intensiver Beschäftigung mit den aktuellen, öffentlich zugänglichen Entwicklungen rund um die europäische Digital-ID sowie die neue EU-Altersverifikations-App bin ich zu dem unumstößlichen Entschluss gekommen, meinen Vertrag nach Ablauf der Mindestvertragslaufzeit nicht fortzuführen.

Ich lehne jede technologische Entwicklung entschieden ab, die dazu führt, dass private Endgeräte der Bürger für staatliche Identitäts-, Verifikations- oder Kontrollfunktionen instrumentalisiert werden. Mein Smartphone ist mein persönliches Eigentum. Ich allein entscheide, welche Anwendungen sich darauf befinden und welchen Zweck sie erfüllen.

Mein Vertrauen in die Unabhängigkeit großer Netzanbieter wurde bereits während der Corona-Zeit nachhaltig erschüttert. Auf meinem eigenen Endgerät befand sich nachweislich die Corona-Warn-Infrastruktur, ohne dass ich einer Installation jemals bewusst zugestimmt hätte. Dieses Erlebnis hat mein Vertrauen in den respektvollen Umgang mit der Privatsphäre von Verbrauchern dauerhaft beschädigt. Ich werde nicht tatenlos abwarten, bis sich diese Form der digitalen Schikane unter dem Deckmantel neuer Verordnungen wiederholt.

Die offiziellen Pläne der EU-Kommission zur Verknüpfung von Internetzugängen mit digitalen Identitätsstrukturen sehe ich in tiefer Sorge vor einer lückenlosen digitalen Überwachung. Ich bin nicht bereit, ein Unternehmen finanziell zu unterstützen, dessen Infrastruktur nach den Erfahrungen der Vergangenheit als tragende Säule für die Umsetzung solcher Kontrollnetzwerke dient.

Aus diesen Gründen kündige ich meinen Vertrag vorsorglich zum nächstmöglichen Ende der Mindestvertragslaufzeit. Bitte bestätigen Sie mir den exakten Kündigungstermin schriftlich innerhalb der gesetzlichen Frist. Von telefonischen oder schriftlichen Rückgewinnungsversuchen bitte ich ausdrücklich Abstand zu nehmen.

Darüber hinaus werde ich meine Beweggründe sowie meine persönliche und journalistische Bewertung dieser Infrastrukturpläne auf meiner eigenen Internetseite veröffentlichen, damit sich auch andere Verbraucher anhand der offiziellen EU-Beweislage ein eigenes Bild machen können.

Mit freundlichen Grüßen,
MAX MUSTERMANN