PrivacyAware zeigt per Ampelsystem, wie stark Websites ihre Besucher verfolgen

BROWSER-ERWEITERUNG MACHT WEBTRACKING SICHTBAR

Cookie-Banner bitten um Zustimmung zu etwas, das sie nicht verständlich erklären. Adblocker blockieren Tracker, machen aber selten transparent, was genau im Hintergrund geschieht. Mit PrivacyAware hat das Institut für Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen eine kostenlose Browser-Erweiterung entwickelt, die Tracking sichtbar macht und Nutzern eine fundierte Entscheidung ermöglicht, bevor sie ihre Daten preisgeben.

Wer eine Webseite aufruft, hinterlässt Spuren. Cookies, Pixel-Tags und Fingerprinting-Verfahren erfassen Klickverhalten, Verweildauer, Suchanfragen und Geräteinformationen. Aus diesen Daten entstehen detaillierte Profile, die Rückschlüsse auf Interessen, Kaufabsichten und politische Einstellungen erlauben. Je präziser ein solches Profil, desto mehr ist es wert: Der globale digitale Werbemarkt soll 2026 rund 712 Milliarden US-Dollar erreichen.[2]

Für die meisten Betroffenen bleiben diese Vorgänge unsichtbar. Viele Onlinedienste wirken kostenfrei, finanzieren sich aber über personalisierte Werbung und datenbasierte Marktanalysen. Webtracking liefert dafür die technische Grundlage. Die eingesetzten Verfahren reichen von einfachen Cookies bis zu komplexen Fingerprinting-Techniken, die Geräte anhand ihrer Hardware- und Software-Konfiguration identifizieren. Welche Daten dabei konkret erhoben, zusammengeführt und weitergegeben werden, erfahren Nutzer in der Regel nicht.

UNTERNEHMEN WISSEN MEHR ALS NUTZER

So entsteht eine strukturelle Informationsasymmetrie: Unternehmen wissen viel über ihre Nutzer – die wissen wenig über die Unternehmen, die ihre Daten verarbeiten. Regulatorische Rahmenbedingungen wie die Datenschutz-Grundverordnung (DSGVO) und das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) setzen dem zwar Grenzen, doch zwischen Rechtsanspruch und Alltagserfahrung klafft eine Lücke. Cookie-Banner fragen nach Einwilligung, erklären aber selten, worin man tatsächlich einwilligt. Datenschutzerklärungen sind umfassend, aber kaum jemand liest sie.

Das Institut für Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen hat nun die Browser-Erweiterung PrivacyAware entwickelt. Sie macht Tracking-Mechanismen sichtbar, bewertet Webseiten nach ihrer Tracking-Intensität und ermöglicht eine informierte Entscheidung, bevor Nutzer ihre Daten preisgeben.

ADBLOCKER BLOCKIEREN, ERKLÄREN ABER NICHT

Auf dem Markt existieren bereits zahlreiche Browser-Erweiterungen, die Werbung und Tracker blockieren. Doch die meisten Adblocker konzentrieren sich auf die technische Blockierung, eine verständliche, vergleichende Transparenz über Art, Umfang und Zweck der eingesetzten Tracking-Verfahren bieten sie kaum. Nutzer erhalten Schutz, jedoch keine Entscheidungsgrundlage.

Hinzu kommt, dass die technische Basis für die Erkennung selbst oft lückenhaft ist. So zeigen aktuelle Untersuchungen, dass viele regionalspezifische Filterlisten die Erwartungen an den Schutz der Nutzer nicht erfüllen. Rund 93 Prozent der darin enthaltenen Regeln erweisen sich in der Praxis als wirkungslos beim Erkennen von Tracking-Anfragen.[6] Selbst wer einen Adblocker einsetzt, kann sich also nicht sicher sein, tatsächlich umfassend geschützt zu werden.

Auch wer technisch geschützt ist, erfährt selten, welche Tracker blockiert wurden, zu welchem Zweck sie Daten erheben wollten und welche Unternehmen dahinterstehen. Dabei setzt Online-Tracking rechtlich eine informierte Einwilligung voraus. Die aus dem Tracking resultierenden Risiken bleiben ebenfalls im Dunkeln – sowohl Privacy-Risiken wie Profilbildung und Re-Identifizierbarkeit als auch Security-Risiken wie Datenlecks oder eine erhöhte Angriffsfläche durch Drittanbieter-Skripte.

COOKIE-BANNER ÜBERFORDERN

Dabei wären informierte Entscheidungen rechtlich geboten. Cookie-Banner sollen genau das ermöglichen. In der Praxis überfordern sie jedoch den Anwender. Komplexe Texte, irreführende Gestaltung und eine hohe Zahl an Auswahlmöglichkeiten führen dazu, dass Nutzer Entscheidungen eher aus Bequemlichkeit treffen als aus Überzeugung. Statt tatsächlicher Kontrolle entsteht lediglich der Eindruck von Mitbestimmung.

Die Zahlen bestätigen das: Eine Bitkom-Studie mit 1.013 Internetnutzern ab 16 Jahren zeigt, dass drei Viertel der Befragten (76 Prozent) von Cookie-Bannern genervt sind. Etwa die Hälfte (51 Prozent) verzichtet auf bestimmte Onlineangebote, weil diese zu viele Cookies verwenden.[3] Viele Menschen bemerken also die Datenerfassung – verstehen oder einordnen können sie diese aber häufig nicht.

Aus dieser Überforderung entsteht, was Forscher als „Privacy Fatigue" bezeichnen: emotionale Erschöpfung, Zynismus oder Hilflosigkeit gegenüber den ständigen Datenschutzanforderungen.[5] Wer permanent entscheiden soll, was er akzeptiert, ohne die Konsequenzen zu verstehen, hört irgendwann auf, sich zu kümmern.

Unsichtbares Tracking wirkt nicht nur technisch, sondern auch psychologisch. Nutzer fühlen sich beobachtet, selbst wenn die Daten anonymisiert erscheinen.[4] Gezielte Werbung und personalisierte Inhalte können Entscheidungen stark beeinflussen – beim Onlineshopping ebenso wie bei der politischen Meinungsbildung. Die permanente Sammlung persönlicher Daten erzeugt Stress, Misstrauen und das Gefühl von Kontrollverlust. Studien belegen, dass Tracking ohne transparente Information zu negativen Emotionen und Verhaltensänderungen führen kann.[1, 5]

Die zentrale Frage lautet daher nicht, ob Tracking stattfindet, sondern ob Nutzer verstehen, was mit ihren Daten geschieht, und auf dieser Basis selbst entscheiden können.

AMPELSYSTEM ZEIGT TRACKING-INTENSITÄT

PrivacyAware setzt an genau dieser Lücke an. Statt Tracker zu blockieren, macht die Browsererweiterung sie sichtbar: Welche Tracking-Technologien setzt eine Webseite ein? Wie intensiv verfolgt sie im Vergleich zu anderen? Und wie datenschutzfreundlich ist sie wirklich?

Das Grundprinzip: Wer eine Webseite aufruft, sieht über ein Ampelsystem auf den ersten Blick, wie stark dort getrackt wird. Grün signalisiert

geringes Tracking, Gelb eine mittlere Ausprägung, Rot warnt vor intensiver Datenerfassung. Die Entscheidung, ob man die Seite trotzdem nutzt, bleibt beim Nutzer. Das Tool trifft somit keine automatisierten Entscheidungen, sondern liefert die Grundlage für eigene.

Ein zentrales Merkmal unterscheidet PrivacyAware von anderen Tools: die präventive Transparenz. Bereits in den Trefferlisten von Suchmaschinen wie Google erscheinen Symbole neben den Links, die das Tracking-Niveau der jeweiligen Seite anzeigen. Nutzer erfahren also nicht erst nach dem Besuch einer Webseite, wie es um deren Datenschutz steht, sondern davor.

Bestehende Privacy-Tools wie Privacy Badger, Ghostery oder uBlock Origin leisten gute Arbeit beim Blockieren von Trackern und Werbung. So erkennt Privacy Badger Tracking-Domains heuristisch und blockiert sie automatisch. Es zeigt Nutzern aber nicht, welche Daten konkret erhoben werden sollten. Ghostery geht einen Schritt weiter und kategorisiert erkannte Tracker nach Unternehmen und Zweck. uBlock Origin arbeitet hocheffizient mit Filterlisten, setzt jedoch vollständig auf Blockierung ohne Transparenzebene. Keines dieser Programme bewertet Webseiten präventiv, bevor man sie aufruft, und keines ermöglicht einen systematischen Vergleich zwischen Webseiten oder Branchen.

Gedacht ist PrivacyAware auch nicht als Konkurrenz zu diesen Werkzeugen, sondern als Ergänzung. Wo Adblocker filtern, soll das Tool einordnen. Wo andere blockieren, schafft es Verständnis.

KOLLEKTIVES WISSEN DURCH GEMEINSAME DATEN

PrivacyAware baut dabei auf einem kollektiven Analyseansatz auf. Wer die Erweiterung nutzt, kann – freiwillig und mit Widerrufsrecht – anonymisierte Tracking-Daten an ein zentrales System übermitteln. Dort fließen sie mit den Ergebnissen automatisierter Scans zusammen, die das System unabhängig von einzelnen Anwendern regelmäßig durchführt. Dabei erfasst das Programm systematisch eingesetzte Tracking-Technologien – besonders Cookies, Fingerprinting-Verfahren und Pixel-Tags – und aktualisiert die Bewertungsgrundlage fortlaufend. So entsteht ein kontinuierlich wachsender Datenpool, von dem alle profitieren.

Damit dieser Pool verlässlich bleibt, gleicht PrivacyAware gespendete Daten technisch mit einer definierten „Ground Truth" ab, also einem Referenzwert aus eigenen Scans. Das reduziert Manipulationsversuche und stellt sicher, dass die Bewertungen auf einer belastbaren Grundlage basieren.

Dieser kollektive Ansatz ermöglicht etwas, das Einzellösungen nicht leisten können: eine vergleichende Betrachtung. Setzen die Webseiten bestimmter Handelsketten systematisch mehr Tracker ein als andere? Wie schneidet eine Branche im Vergleich ab? Die Ergebnisse sind über eine eigene Webseite öffentlich zugänglich. Dort entsteht ein Ranking, das aus dem aktuellen Bestand geprüfter Domains sowohl die fünf mit der geringsten als auch die fünf mit der höchsten Tracking-Intensität ausweist. So werden strukturelle Unterschiede im Umgang mit Nut-

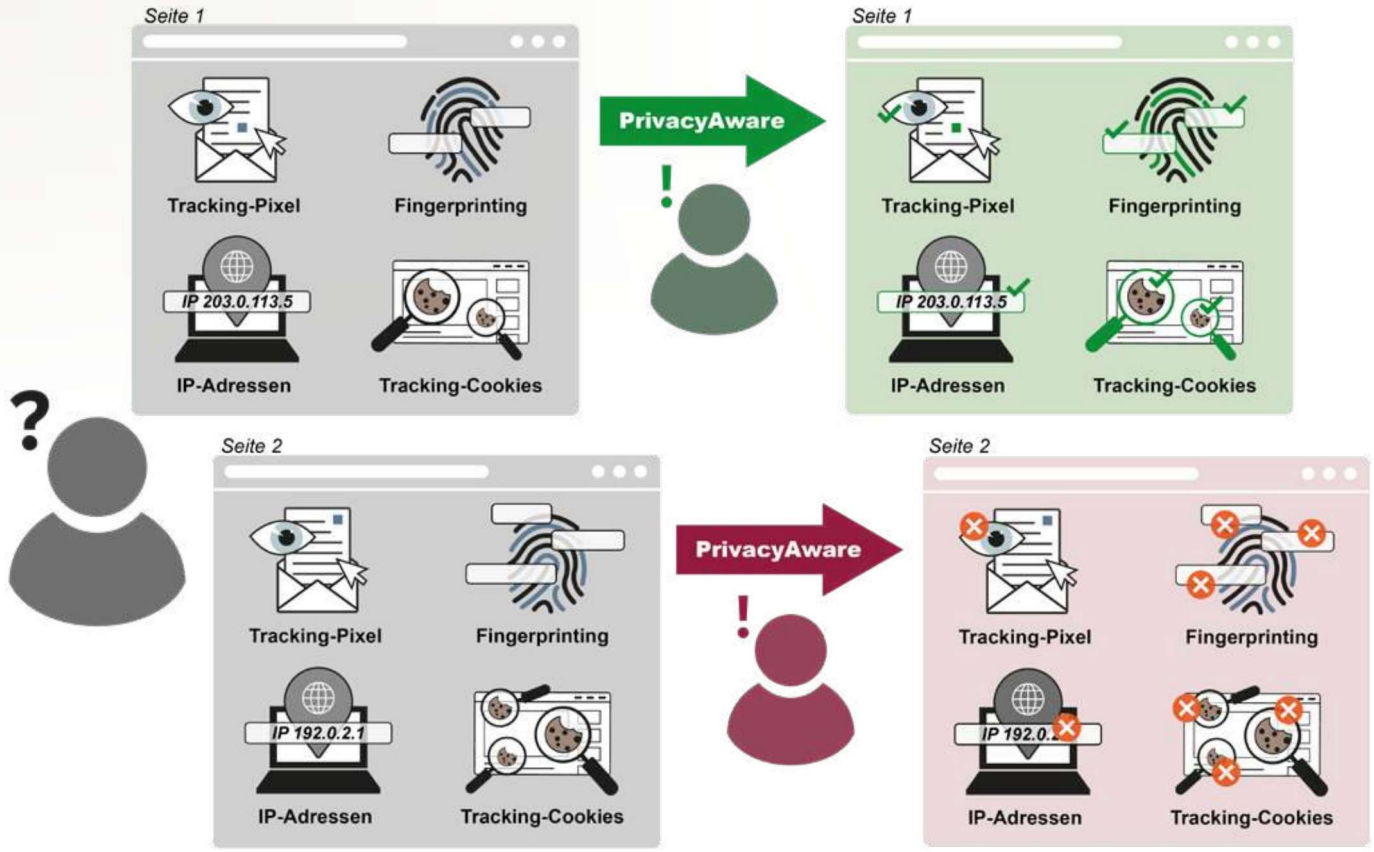

Abbildung 1: PrivacyAware (Bild: if(is))

zerdaten sichtbar – über den Einzelfall hinaus und für jeden einsehbar.

Neben der Tracking-Analyse prüft die Erweiterung auch, ob eine Domain potenziell schädliche Inhalte enthält, etwa Malware, Phishing oder betrügerische Angebote. Sie verbindet so Datenschutz-Transparenz mit grundlegender Sicherheitsinformation.

FÜR ALLE NUTZER GEDACHT

Mit PrivacyAware richten sich die Entwickler an alle, die das Internet nutzen, unabhängig vom technischen Vorwissen. Ferner kann es Aufsichtsbehörden und Datenschutzbeauftragten bei Prüfungen helfen, indem es Tracking-Technologien sichtbar macht und kritische Passagen in Datenschutzerklärungen hervorhebt. Das Browser-Add-on ist ein Angebot des Instituts für Internet-Sicherheit[7] und wird zusätzlich über den Marktplatz IT-Sicherheit[8] bereitgestellt. Das Projekt verfolgt keinen kommerziellen Zweck. Ziel ist es, möglichst vielen Menschen einen informierten Umgang mit dem Internet zu ermöglichen.

Darüber hinaus soll PrivacyAware von Behörden, Initiativen und Verbänden unterstützt und verbreitet werden. Ein sichereres Internet entsteht nicht allein durch individuelle Maßnahmen. Es braucht kollektive Ansätze, um Transparenzstandards zu stärken, Vergleichbarkeit zu ermöglichen und Anreize für eine datenschutzfreundlichere Gestaltung von Onlineangeboten zu schaffen.

FUNKTIONEN IM DETAIL

PrivacyAware untersucht jede Webseite auf drei zentrale Tracking-Technologien – Cookies, Fingerprinting und Pixel-Tags –, bewertet deren Eingriffsintensität und verdichtet die Ergebnisse zu einer Gesamteinschätzung. Ergänzend analysiert es Datenschutzerklärungen und prüft Domains auf Sicherheitsrisiken. Im Folgenden ein Blick auf die einzelnen Bausteine.

COOKIES NACH EINGRIFFSINTENSITÄT GEWICHTET

Cookie ist nicht gleich Cookie. PrivacyAware erkennt die auf einer Webseite gesetzten Cookies und ordnet sie auf Basis der Referenzdatenbank Cookiepedia automatisch Kategorien zu:

- **Strictly Necessary:** technisch erforderlich für die Grundfunktion der Webseite
- **Functionality:** Komfortfunktionen wie Spracheinstellungen oder Layout-Präferenzen
- **Performance:** Analyse und Optimierung der Webseite
- **Targeting/Advertising:** Werbung und Profilbildung
- **Unknown:** Zweck unklar
- **No Data:** keine Informationen verfügbar

Entscheidend ist dabei, dass die Browser-Erweiterung Cookies nicht einfach zählt, sondern sie nach ihrer Eingriffsintensität gewichtet. Cookies aus den Kategorien Targeting und Advertising fließen am stärksten in die Bewertung ein, weil sie der Profilbildung und verhaltensbasierten Analyse dienen. Auch manche Performance-Cookies, etwa von Google, dienen dem Tracking und erhalten eine höhere Gewichtung. Nicht klassifizierte und unbekannte Cookies stuft das Tool als potenziell risikobehaftet ein. Technisch notwendige Cookies dagegen fließen kaum in die Bewertung ein.

Damit unbekannte Cookies nicht dauerhaft als Risiko gewertet werden, kommen zwei Mechanismen zum Einsatz: Dynamische Mustererkennung (Regex) ordnet technisch bedingte, variierende Cookie-Namen korrekt zu. Zusätzlich gleicht die Erweiterung unbekannte Cookies kontinuierlich über die Cookiepedia-API ab und korrigiert die Einstufung, sobald neue Informationen vorliegen.

FINGERPRINTING ERKENNEN

Fingerprinting gehört zu den invasivsten Tracking-Methoden, und zu den unsichtbarsten. Anders als Cookies lässt es sich nicht einfach löschen, weil es keine Daten auf dem Gerät speichert. Stattdessen identifiziert es Nutzer anhand der individuellen Kombination von Hardware- und Softwaremerkmalen ihres Gerätes.

PrivacyAware analysiert den geladenen JavaScript-Stack einer Webseite heuristisch und erkennt dabei fünf Fingerprinting-Kategorien:

- **Canvas-Fingerprinting** identifiziert Geräte über unsichtbare Grafik-Renderings im Browser.
- **WebGL-Fingerprinting** wertet 3D-Grafikverarbeitung und Treiberinformationen aus.
- **Audio-Fingerprinting** erkennt Geräte anhand der Signalverarbeitung über die Web Audio API.
- **Font-Fingerprinting** analysiert installierte und darstellbare Schriftarten.
- **Media-Device-Fingerprinting** erfasst angeschlossene Geräte wie Kamera oder Mikrofon.

Die Bewertung erfolgt über ein gewichtetes Punktesystem, das die Eingriffstiefe widerspiegelt. WebGL-Fingerprinting erhält mit drei Punkten die höchste Gewichtung, weil es tiefgreifende Systeminformationen einbezieht. Canvas- und Audio-Fingerprinting liegen mit je zwei Punkten im Mittelfeld. Browsernahe Verfahren wie Font- und Media-Device-Erkennung fließen als Basis-Identifikatoren mit einem Punkt ein.

PIXEL-TAGS ZÄHLEN

Pixel-Tags – auch Zählpixel oder Tracking-Pixel genannt – sind winzige, unsichtbare Bilddateien, die beim Laden einer Webseite eine Verbindung zu einem Server aufbauen und so den Besuch registrieren. Die Erweiterung erkennt diese Pixel dynamisch: Beim Seitenaufruf erfasst sie die zunächst eingebundenen Pixel, bei Interaktionen wie Scrollen registriert sie nachladende Elemente.

Die erkannten Pixel-Tags unterscheidet das Tool nach First-Party- und Third-Party-Elementen. Eine erhöhte Anzahl gilt als Indikator für höhere Tracking-Intensität und fließt als normierter Teilscore in die Gesamtbewertung ein – allerdings mit geringerer Gewichtung als Cookies und Fingerprinting.

GRÜN, GELB ODER ROT

Alle Analyseergebnisse – Cookies, Fingerprinting, Pixel-Tags – fließen in ein Ampelsystem ein, das die Tracking-Intensität einer Webseite auf eine Farbe verdichtet: Grün bedeutet geringes Tracking – Nutzung aus Datenschutzsicht unkritisch. Gelb bedeutet mittleres Tracking – erhöhte Aufmerksamkeit empfohlen. Rot bedeutet intensives Tracking – Besuch aus Datenschutzperspektive nicht empfohlen.

Die Ampelfarben sind eine Empfehlung, keine Sperre. Wer eine rot bewertete Seite trotzdem besuchen will, kann das jederzeit tun. Das

Ampelsystem hilft, Risiken schnell zu erfassen, ohne sich durch technische Details arbeiten zu müssen.

Darüber hinaus bietet PrivacyAware drei weitere Funktionen:

- **Datenschutzerklärungen auf den Punkt bringen:** Kaum jemand liest Datenschutzerklärungen vollständig. PrivacyAware übernimmt die Vorarbeit: Die Funktion „Privacy Critics" durchsucht die Datenschutzerklärung einer Webseite nach potenziell kritischen Begriffen wie „Weitergabe", „Dritte" oder „Profiling". Die entsprechenden Sätze extrahiert die Erweiterung, hebt die Schlüsselwörter fett und rot hervor und zeigt sie übersichtlich an. Ergänzend visualisiert das Tool die kritischen Begriffe durch standardisierte Datenschutz-Icons. Diese ikonografische Darstellung reduziert komplexe Inhalte auf das Wesentliche und macht zentrale Aspekte der Datenverarbeitung schnell erfassbar – ohne dass man die vollständige Erklärung lesen muss.

- **Schutz vor schädlichen Webseiten:** Über die Schnittstelle zu Google Safe Browsing prüft PrivacyAware beim Aufruf einer Webseite, ob deren Adresse auf einer aktuellen Bedrohungsliste steht, etwa wegen Phishing, Malware oder betrügerischer Inhalte. Dabei wird lediglich ein verkürzter Hash der URL übermittelt, die Privatsphäre bleibt also gewahrt.

- **Blacklist und Whitelist:** Das Tool bietet ein integriertes Filtersystem, mit dem Nutzer problematische Domains präventiv blockieren können. Die Blacklist umfasst Kategorien wie Glücksspiel, Fake News, Adult Content, Social Media sowie bekannte Tracking- und Werbedomains. Die Whitelist ermöglicht es, zuvor blockierte Domains gezielt wieder freizugeben. Zusätzlich lassen sich eigene Domainlisten im TXT-Format hochladen – für individuelle Kontrolle über den eigenen Webzugang.

TRANSPARENZ ALS GRUNDLAGE FÜR VERTRAUEN

Webtracking ist ein struktureller Bestandteil der digitalen Ökonomie. Trotz regulatorischer Rahmenbedingungen bleibt die tatsächliche Datenverarbeitung für viele Nutzer intransparent. Die im Beitrag dargestellten Befunde und Studien zeigen: Rein formale Einwilligungsmechanismen reichen häufig nicht aus, um informierte Entscheidungen zu ermöglichen. Phänomene wie Privacy Fatigue machen deutlich, dass fehlende Verständlichkeit und kognitive Überlastung zentrale Hindernisse für die digitale Selbstbestimmung sind.

Transparenz im Umgang mit Tracking-Mechanismen und personenbezogenen Daten bleibt deshalb eine Grundvoraussetzung für die digitale Selbstbestimmung. Wer digitale Dienste langfristig akzeptieren soll, muss ihnen vertrauen können. Transparenz schafft dieses Vertrauen, weil sie informierte Entscheidungen ermöglicht und Informationsasymmetrien reduziert.

PrivacyAware verfolgt deshalb keinen primär blockierenden, sondern einen transparenzorientierten Ansatz. Die systematische Erkennung von Cookies, Fingerprinting-Techniken und Pixel-Tags, die strukturierte Kategorisierung, das Ampelsystem und der branchenbezogene Vergleich machen Tracking nicht nur technisch sichtbar, sondern auch einordbar und vergleichbar. Die visuelle Aufbereitung von Datenschutzerklärungen reduziert zusätzlich die kognitive Belastung.

Der Mehrwert für die Benutzer liegt in der Verbindung von technischer Analyse und verständlicher Darstellung. So entsteht eine belastbare Grundlage für fundierte Entscheidungen im digitalen Raum. ■

Literaturverzeichnis

[1] *Sivan-Sevilla, I., & Poudel, P. (2024). Web privacy based on contextual integrity: Measuring the collapse of online contexts. arXiv. https://arxiv.org/abs/2412.16246*

[2] *Global Market Statistics. (2026). Digital advertising market size, share, growth and industry forecast: Global digital advertising market report. https://www.globalmarketstatistics.com/de/market-reports/digital-advertising-market-12281*

[3] *Bitkom Research. (2024, 25. März). Drei Viertel sind von Cookie-Bannern genervt. Bitkom Research. https://bitkom-research.de/news/drei-viertel-sind-von-cookie-bannern-genervt*

[4] *Coopamootoo, K. P. L., Mehrnezhad, M., & Toreini, E. (2022). "I feel invaded, annoyed, anxious and I may protect myself": Individuals' feelings about online tracking and their protective behaviour across gender and country. arXiv. https://arxiv.org/abs/2202.04682*

[5] *van der Schyff, K., Foster, G., Renaud, K., & Flowerday, S. (2023). Online privacy fatigue: A scoping review and research agenda. Future Internet, 15(5), Article 164. https://doi.org/10.3390/fi15050164*

[6] *Böttger, T., et al. (2025). Understanding regional filter lists: Efficacy and impact. Proceedings on Privacy Enhancing Technologies (PoPETs), 2025(2), 309–325. https://doi.org/10.56553/popets-2025-0063*

[7] *Institut für Internet-Sicherheit: https://internet-sicherheit.de/*

[8] *Marktplatz IT-Sicherheit: https://it-sicherheit.de/*

BARYALAI USMANI
studiert im Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit „Privatsphäre im Internet und Security Awareness".

CHRISTIAN BÖTTGER
ist Doktorand im Themenschwerpunkt „Privatsphäre im Internet" im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen

OLIVER SCHONSCHEK
ist wissenschaftlicher Mitarbeiter mit dem Forschungsschwerpunkt „IT-Sicherheit für KMUs" im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen.

NORBERT POHLMANN
ist Professor für Cybersicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.