Martin Degeling, Christine Utz, Tobias Urban

Effekte der DSGVO auf Webseiten und die Entwicklung der ePrivacy-Verordnung

Die europäische Datenschutz-Grundverordnung wurde für viele Bürger*innen vor allem durch vermehrte Einverständniserklärungen auf Webseiten und in der Online-Kommunikation sichtbar. Dabei behandelt die Verordnung den Online-Bereich nur am Rand, sollte er doch durch eine parallel erlassene ePrivacy-Verordnung reguliert werden – die bis heute nicht verabschiedet wurde. Welche Auswirkungen die DSGVO dennoch auf Webseiten und deren Besucher*innentracking hatte, haben die Autor*innen mit Online-Tests ermittelt, wie sie im folgenden Beitrag beschreiben.

1 Einleitung

Die Datenschutz-Grundverordnung (DSGVO) gilt als großer Wurf in der europäischen Gesetzgebung. Sie vereinheitlicht das – global gesehen – hohe Datenschutzniveau innerhalb der EU und setzt mit dem Marktortprinzip einheitlich Standards auch für transnational organisierte Daten-Plattformen. Von Seiten der Datenschützer:innen und Aktivist:innen waren daher auch von Anfang an hohe Erwartungen an die DSGVO geknüpft, nicht zuletzt in Bezug auf lange bestehende und häufig kritisierte Datensammlungen im Internet zu Marketingzwecken. Im Zuge der Kommerzialisierung vieler Webseiten und der Fokussierung vieler Online-Dienste auf Werbeeinnahmen hat sich in den letzten 20 Jahren eine Infrastruktur etabliert, mittels derer immer detailliertere Profile von Personen erstellt und ausgetauscht werden (Turow 2012).

Zwei Jahre nach der Einführung der DSGVO ist das datenintensive Online-Tracking allerdings immer noch weit verbreitet – auch weil die DSGVO Datenschutz im Internet nur am Rande behandelt und die genaue Regulierung einer ePrivacy-Verordnung überlassen werden sollte (siehe dazu Glatzner 2018). Diese sollte kurz nach der DSGVO

Zitiervorschlag:
Degeling, Martin; Utz, Christine; Urban, Tobias (2020): Effekte der DSGVO auf Webseiten und die Entwicklung der ePrivacy-Verordnung, vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik Nr. 231/232 [59(3-4)], S. 77-86.

verabschiedet werden, verzögert sich aber weiter. Aktuell ist der Online-Datenschutz daher gefangen zwischen der Lobbyarbeit der Internet- und Marketingindustrie, die den Status quo bestenfalls erhalten will, und einer sich teilweise widersprechenden und zumindest unklaren Gesetzeslage zwischen der DSGVO und dem Telemediengesetz.

Seit 2017 haben wir mehrere Studien durchgeführt, um die Auswirkungen der DSGVO und die Umsetzung datenschutzfreundlicher Praktiken im Internet zu untersuchen. In diesem Beitrag wollen wir einige Ergebnisse unserer Arbeit vorstellen und zeigen, dass viele Webseiten zwar genauer über ihre Datenverarbeitung informieren und Nutzer:innen teilweise Entscheidungsmöglichkeiten einräumen, die negativen Effekte für die Privatheit der Betroffenen in der Breite aber kaum zurückgegangen sind. Stattdessen konsolidiert sich die Tracking-Branche und Nutzer:innen zeigen sich von oft wirkungslosen Cookie-Hinweisen genervt. Während sich die ePrivacy-Verordnung weiter verzögert, versuchen Lobbygruppen der Werbeindustrie und Browserhersteller:innen, neue Standards zu entwickeln und durchzusetzen.

2 Tracking zu Werbezwecken

Seit 1994 das erste Werbebannner auf einer Webseite eingebunden wurde, wächst die Online-Marketing-Branche kontinuierlich. Neben den Umsätzen steigt auch die Menge der personenbezogenen Daten, die zur Personalisierung und Optimierung von Werbeanzeigen gesammelt, verarbeitet und ausgetauscht werden. Seit einigen Jahren prägen Begriffe wie *Real Time Bidding* (Busch 2014) und *Programmatic Advertising* (Bundesverband Digitale Wirtschaft (BVDW) e.V. 2017) die Branche. Sie beschreiben vor allem die Technisierung und Automatisierung der Zusammenarbeit zwischen denen, die Werbung schalten wollen (Demand-Side-Plattform), und denen, die Werbeplätze auf ihren Webseiten oder in Videos anbieten (Supplier-Side-Plattform). Dazwischen hat sich ein unübersichtliches Geflecht an Unternehmen positioniert, das automatisiert zwischen den beiden Seiten vermittelt. Besucht man heutzutage eine Webseite, steht zu Beginn noch nicht fest, welche Werbung angezeigt wird, sondern nur Anzahl und Position der Werbeflächen. Abhängig vom Inhalt der Seite, vor allem aber auch von Informationen über den:die Besucher:in, wird die Fläche auf Supplier-Side-Plattformen angeboten und automatisiert entschieden, welche Werbekampagne auf einer Demand-Side-Plattform bereit ist, den höchsten Preis zu zahlen. Dieses „*Targeted Advertising*“ manifestiert sich in dem bekannten Phänomen, sich von Werbung für ein Produkt „verfolgt“ zu fühlen und wiederholt auf Seiten Werbung dafür zu sehen, nur weil man vor einiger Zeit danach gesucht hat. Im Zentrum dieser Transaktionen stehen pseudonyme Profile, an die Informationen über (Kauf)interessen und demographische Informationen gekoppelt sind. Das zum Oracle-Konzern gehörende Online-Marketing-Unternehmen Bluekai etwa hatte 2018 ein Kategoriensystem, das 786 verschiedene Interessen abbildete (Degeling and Nierhoff 2018). Der Internetgigant Google klassifiziert in 1024 Interessen (Degeling 2017). Technisch realisiert wird das Online-Profiling hauptsächlich über Cookies - eine Eigenschaft des HTTP-Protokolls, auf die sich das

Internet stützt: Sie erlaubt es Webseitenbetreiber:innen, kurze Textschnipsel im Browser der:s Nutzer:in abzuspeichern und später wieder abzurufen. Auf diese Weise kann eine Wiedererkennung umgesetzt werden, etwa um den aktuellen Login-Status oder in den Warenkorb eines Online-Shops gelegte Produkte zu speichern. Gleichsam ist damit jedoch auch eine Nachverfolgung zur Profilbildung für Werbezwecke möglich.

3 Einfluss der DSGVO auf Werbenetzwerke

Die möglichen Auswirkungen der DSGVO auf Online-Werbung wurden vor ihrer Einführung intensiv diskutiert. Industrienahe Gruppen und Verbände haben im Vorfeld den „Untergang" der Online-Werbung prophezeit (Scott 2017; Ward 2017). In unterschiedlichen Forschungsarbeiten konnte allerdings gezeigt werden, dass infolge der DSGVO nicht signifikant weniger (Werbe-)Dienste in Webseiten eingebunden werden, wohl aber im Vergleich zu US-Webseiten in Europa weniger Tracking-Dienste zum Einsatz kommen (WhoTracksMe 2018; Sørensen and Kosta 2019). Eine Folge der Einführung der DSGVO ist, dass Werbetreibende mit hohen Marktanteilen ihre Position festigen oder sogar weiter ausbauen konnten und kleine Unternehmen vom Markt verschwunden sind beziehungsweise Anteile verloren haben. Die DSGVO hat somit zu einer Konsolidierung des Marktes geführt (Johnson, Shriver, and Goldberg 2020; Solomos et al. 2019). Für Nutzer:innen bedeutet dies konkret, dass nun zwar weniger Unternehmen ihre Online-Aktivitäten verfolgen, diese aber dafür auf mehr Webseiten präsent sind und somit ihr Surfverhalten in größerem Umfang beobachten können.

In einer Studie im Jahr 2018 haben wir das Ausmaß der Konsolidierung und der Reichweite einzelner Trackingdienste anhand von „*Cookie Syncing*" untersucht. Dabei handelt es sich um eine Praxis, bei der zwei oder mehr Werbetreibende Identifikatoren von Benutzer:innen, gespeichert in Cookies, untereinander austauschen und anschließend weitere ihnen über diese Nutzer:innen vorliegende Daten untereinander austauschen (Papadopoulos, Kourtellis, and Markatos 2018). Über diesen Datenabgleich können die einzelnen Unternehmen eine größere Datenbasis aufbauen und die Algorithmen zur Ermittlung der Werbeanzeigen optimieren. Während wie oben beschrieben die durchschnittliche Anzahl von Trackern auf einer Website nur leicht zurückgegangen ist, konnten wir zeigen, dass die DSGVO einen Einfluss auf das „*Cookie Syncing*" hat und dieses statistisch signifikant zurückgegangen ist (Urban et al. 2020). Abbildung 1 zeigt exemplarisch die Veränderungen in der Vernetzung der Dienste. Links wird ein Teil des Netzwerks vor Einführung der Verordnung dargestellt und rechts einige Tage nach dem Inkrafttreten am 25. Mai 2018. Es ist zu erkennen, dass weniger dritte Parteien (Knoten) und Verbindungen zwischen diesen (Kanten) existieren. Allerdings hat sich dabei die grundlegende Struktur des gesamten Netzwerks nicht verändert. Google bleibt z. B. weiterhin der wichtigste Datenumschlagsplatz. Unsere Ergebnisse legen nahe, dass die DSGVO nicht zu einer grundsätzlichen Änderung oder nachhaltigen Störung in den Werbenetzwerken geführt hat.

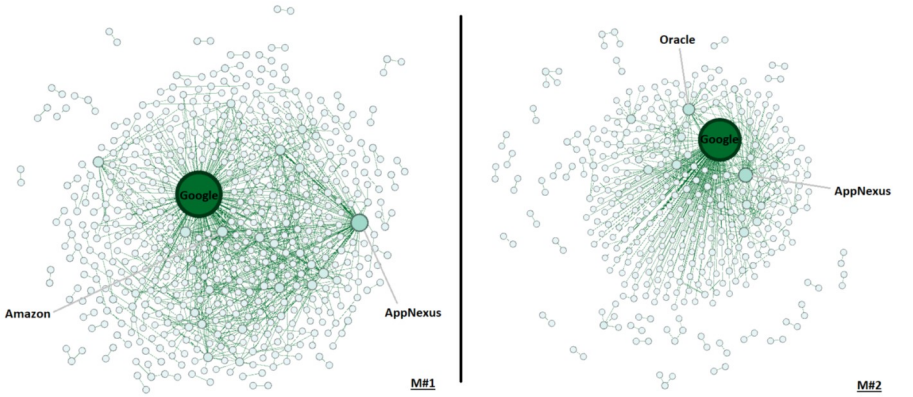

Abbildung 1: Die Graphen zeigen die Veränderung im Werbenetzwerk nach Einführung der DSGVO. Die Knoten stellen die einzelnen Unternehmen dar und die Kanten die Verbindungen („*Cookie Syncing*“) zwischen ihnen. Je größer ein Knoten ist, desto besser ist er in dem Netzwerk verbunden.

4 Einfluss der DSGVO auf Webseiten

Jenseits des Trackings haben wir auch untersucht, wie Webseiten ihre Datenschutzinformationen und Datenverarbeitungspraktiken geändert haben (Degeling et al. 2019).

Dazu haben wir die 500 beliebtesten Webseiten in jedem EU-Mitgliedsstaat, insgesamt 6579 Seiten, im Zeitraum von Dezember 2017 bis August 2018 beobachtet. Durch wiederholte, automatisierte Webseitenaufrufe ließ sich die Entwicklung dieser Seiten und ihrer datenschutzrelevanten Eigenschaften verfolgen. Dazu gehörte neben dem Vorhandensein einer Datenschutzerklärung auch der Einsatz von Informations- bzw. Zustimmungsdialogen.

Diese Messungen zeigen, dass Webseiten trotz der 24-monatigen Übergangsfrist zur Umsetzung der DSGVO erst zu deren Ende aktiv geworden sind und Bestrebungen zur Umsetzung der neuen Regeln unternommen haben. Grafik 2 verdeutlicht, dass über 75 % der Webseiten ihre Datenschutzerklärung erst 2018 überarbeitet haben, die Mehrheit sogar erst im Mai Änderungen vorgenommen hat. Nicht in diese Analyse eingeflossen sind hier die 10,5 % der 6357 untersuchten Webseiten, die auch nach Einführung der DSGVO ihren Besucher:innen keine Datenschutzinformationen anbieten.

Bezüglich der Länge der untersuchten Datenschutzerklärungen war ein knapp 42 %-iger Anstieg der durchschnittlichen Wortanzahl zu verzeichnen, von 2145 Wörtern im März 2018 zu 3044 im Mai 2018. Die Ursache hierfür kann in den neuen Transparenzanforderungen der Art. 13 f. DSGVO gesehen werden. Ob diese so das Anliegen der DSGVO verwirklichen können, den Nutzer:innen die Verarbeitung ihrer persönlichen Daten leichter verständlich zu machen, darf zumindest angezweifelt werden.

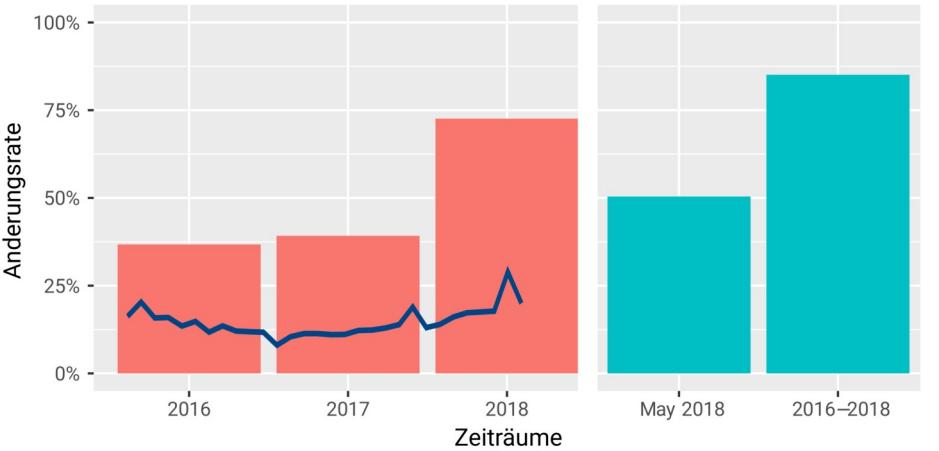

Abbildung 2: Der Graph zeigt die Rate der Änderungen in Datenschutzerklärungen über die Zeit (Linie) und in verschiedenen Zeitabschnitten (rote Balken). Die blauen Balken zeigen, wie viel Prozent der Datenschutzerklärungen auf den untersuchten Webseiten in dem genannten Zeitraum eine Änderung erfahren haben.

Im Verlauf dieser Studie fiel ferner auf, dass mehr und mehr Webseiten sogenannte „Cookie-Banner" einsetzten, d. h. Dialogfenster, die die Besucher:innen der Webseite über deren Einsatz von Cookies und ähnlichen Tracking-Technologien informieren und gegebenenfalls um Zustimmung zu deren Einsatz bitten. Eine Pflicht der Webseiten, zum Abspeichern technisch nicht zwingend notwendiger Cookies im Browser der Besucher:innen deren Zustimmung einzuholen, sieht bereits Artikel 15 der im Jahr 2009 novellierten ePrivacy-Richtlinie vor. Doch auch Zustimmung als Rechtsgrundlage gemäß Art. 6 Abs. 1 (a) DSGVO scheint Webseiten zum Einsatz von Cookie-Bannern zu veranlassen – im Januar 2018 konnte auf 46,1 % der untersuchten Seiten ein solches Banner gefunden werden und nach dem Inkrafttreten der DSGVO auf 62,1 % der Webseiten.

Der Großteil der gefundenen Banner bietet den Nutzer:innen jedoch keine Möglichkeit, dem Einsatz von Cookies und Tracking-Technologien zu widersprechen, sodass nicht von einer „freien" Entscheidung im Sinne der DSGVO gesprochen werden kann. Demgegenüber ließ sich unter den Bannern, die Optionen zur Abwahl bieten, eine Zunahme der Komplexität beobachten: Neben Bannern, die eine schlichte An- oder Abwahl aller Cookies erlauben, fanden sich auch zunehmend welche, bei denen dies für einzelne Kategorien von Diensten (z. B. soziale Medien, Nutzungsanalyse oder Marketing) oder gar jede einzelne Drittpartei individuell möglich ist. Oft sind solche detaillierten Auswahlmöglichkeiten jedoch nicht auf den ersten Blick ersichtlich, sondern werden hinter schwer erkennbaren Links versteckt, während die Option zum Akzeptieren aller Cookies grafisch hervorgehoben ist. Dies ist ein Beispiel für die bei Cookie-Bannern verbreiteten sogenannten Dark Patterns, d. h. bewusste Designent-

scheidungen mit dem Ziel, die Nutzer:innen zur Vornahme einer gewissen Handlung – hier der Zustimmung zur Verwendung aller Cookies – zu bewegen (Soe et al. 2020).

In einer Anschlussstudie untersuchten wir diese Zustimmungsdialoge bzw. Cookie-Banner genauer, um zu verstehen, ob und wie Nutzer:innen mit ihnen interagieren und welche Vorstellungen von den dahinterstehenden Mechanismen sie haben (Utz et al. 2019).

Hierfür haben wir auf einer deutschen eCommerce-Website iterativ verschiedene Cookie-Banner geschaltet, die sich jeweils in ein bis zwei Interface-Eigenschaften unterschieden, wie der Position oder der Anzahl der angebotenen Optionen sowie dem Einsatz von Dark Patterns. Es zeigte sich, dass am häufigsten mit Zustimmungsdialogen in der linken unteren Ecke des Bildschirms interagiert wird, möglicherweise weil Dialoge dort aufgrund von Layout und Textfluss eher wichtigen Inhalt der Website verdecken. Ferner ließ sich ein signifikanter Einfluss der Verwendung von Dark Patterns ausmachen: Banner, bei denen Zustimmung signalisierende Buttons farblich herausgestellt oder Kästchen zur Auswahl zuzulassender Kategorien oder Drittparteien vorangekreuzt waren, wiesen höhere Interaktions- und Zustimmungsraten auf als diejenigen ohne den Einsatz dieser Techniken. Das in einem Anschlussfragebogen von den Besucher:innen der Website gesammelte Feedback legte nahe, dass eine einfache Ja-Nein-Entscheidung sowie kategorienbasierte Banner bevorzugt werden. Es zeigten sich aber auch weit verbreitete Fehleinschätzungen bezüglich der Funktionsweise von Cookies und Cookie-Bannern: Ein häufig genannter Grund für eine Interaktion mit dem Banner war die Erwartung, dass die Website ohne Zustimmung überhaupt nicht genutzt werden könnte.

Es gibt in der Praxis einige Cookie-Banner, die von Nutzer:innen durch Blockieren der darunterliegenden Website eine Zustimmung erzwingen oder bei einem Klick auf „Ablehnen“ auf ihre Datenschutzerklärung oder Drittseiten wie Google umleiten und ihnen so die weitere Nutzung der Seite verwehren. Dieses Verhalten könnte hier die Wahrnehmung der Befragten entsprechend beeinflusst haben, während korrekt implementierte und die getroffene Auswahl respektierende Banner nur Funktionseinschränkungen der betroffenen Seite zur Folge haben sollten. Dass Letzteres in der Realität nicht vorausgesetzt werden kann, zeigt eine jüngst veröffentlichte Studie zu den weit verbreiteten Bannern auf Grundlage des IAB Europe *Transparency and Consent Framework* (TCF)[1], nach der Seiten teilweise eine verweigerte Zustimmung wie eine erteilte behandeln oder bereits vor Auswahl einer Option durch die Besucher:innen Cookies gesetzt werden (Matte, Bielova, and Santos 2020). Einen dementsprechenden Eindruck hatten auch einige der Befragten in unserer Studie, die auf die Frage danach, weshalb sie mit dem Banner nicht interagiert hatten, antworteten, es mache ohnehin keinen Unterschied, welche der angebotenen Optionen ausgewählt werde. Während Zustimmungsdialoge eigentlich als Transparenzmechanismus gedacht sind, scheint es ihnen derzeit gerade an dem dafür essenziellen Vertrauen der Nutzer:innen zu mangeln, bedingt durch unklare oder uneinheitliche Vorgaben und mangelhafte Implementierung durch die Webseiten.

5 Aktuelle Entwicklungen im Online-Tracking

Während zuletzt in einem Urteil die Pflicht zur informierten und getrennten Einwilligung bestätigt wurde (z. B. EuGH v. 1.10.2019 – C-673/17 – Planet49), tut sich in der Praxis weiterhin wenig. Mehrere Vorstöße, eine ePrivacy-Verordnung auf den Weg zu bringen, sind wieder eingeschlafen. Nach Informationen einer Webseite, die DSGVO-bezogene Bußgelder auflistet, sind bisher nur spanische Datenschutzaufsichtsbehörden aktiv geworden.[2] In Deutschland wollen die Landesbeauftragten laut Medienberichten vom August 2020 (Kleinz 2020) ein Jahr nach der Veröffentlichung von Empfehlungen durch die Datenschutzkonferenz in Kürze beginnen, vor allem Medienhäuser auf die Einhaltung der Vorgaben zu prüfen.

Eine detaillierte gesetzliche Grundlage in Deutschland könnte, unabhängig von der ePrivacy-Verordnung, bald durch das „Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)“ geschaffen werden. In einer ersten Analyse des Referent:innenentwurfs aus dem BMWI identifiziert Härting (Härting 2020) gegenüber den geltenden Vorgaben zwei Öffnungsklauseln: in § 9 Abs. 2 TTDSG-RefE, der die Nutzung von Cookies (jenseits der Einwilligung) im Rahmen vertraglicher Verpflichtungen ermöglichen würde, sowie in § 9 Abs. 4 TTDSG-RefE, wenn explizite Browsereinstellungen dies ermöglichen. Statt Einwilligungen jeweils einzeln und für jede Webseite spezifisch geben zu müssen, könnten Benutzer:innen über Dialoge in ihren Browsern einmalig festlegen, welchen Formen von Cookies und Tracking sie zustimmen. Dies setzt allerdings eine einheitliche Kategorisierung der Zwecke des Einsatzes von Cookies voraus, an der aktuell viele Webseiten scheitern (Fouad et al. 2020).

Auf der Seite der Nutzer:innen positionieren sich insbesondere die Browserhersteller:innen und setzen sich für mehr Datenschutz ein. Neben dem explizit auf Datenschutz ausgerichteten Browser Brave haben auch Firefox und Safari zunehmend technische Beschränkungen für Tracking und Cookies implementiert. Sogar Chrome, entwickelt von Google, dessen Haupteinnahmequelle im Schalten von personalisierter Werbung besteht, will sich zukünftig von Third-party-Cookies trennen. Allerdings ist davon auszugehen, dass dies nicht das Ende des Online-Trackings sein wird, sondern andere, nicht auf Cookies basierende Techniken zum Einsatz kommen werden. Zu diesen gehört etwa Browser-Fingerprinting, bei dem Nutzer:innen anhand von charakteristischen Eigenschaften ihrer Soft- und Hardwarekonfiguration wiedererkannt werden.

In der Forschung wurde zuletzt wiederholt gezeigt, dass Online-Werbung weniger Vorteile hat als häufig versprochen wird. So zeigten Frik et al., dass die Nachteile der Nutzung von Ad-Blockern für Internetnutzer:innen gering sind (Frik, Haviland, and Acquisti 2020). Zuvor hatte dieselbe Forschungsgruppe belegt, dass personalisierte Werbeanzeigen nur wenig monetäre Vorteile gegenüber nicht personalisierter Werbung bieten (Marotta, Abhishek, and Acquisti 2019). Vielmehr zeigen Fallstudien (Edelman 2020), dass Webseiten mit Anzeigen abhängig vom Kontext höhere Einnahmen erzielen können. Statt einer Fortführung der langen Auseinandersetzung zwischen Werbetracking und Datenschutz könnte sich am Ende auch die Erkenntnis

durchsetzen, dass datenschutzfreundlichere Werbung, die ohne Nutzer:innenprofile funktioniert, für alle Seiten Vorteile hat.

MARTIN DEGELING ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Systemsicherheit des Horst Görtz Instituts für IT Sicherheit der Ruhr-Universität Bochum. Er promovierte 2016 an der Universität Duisburg-Essen zum Thema „Online Profiling". Im Anschluss hat er an der Carnegie Mellon University zu *usable privacy and security* und dem Internet der Dinge geforscht. Zuletzt war er an mehrere Studien beteiligt, die die Auswirkungen der Datenschutzgrundverordnung auf Webseiten untersucht haben.

CHRISTINE UTZ hat Rechtswissenschaften und IT-Sicherheit studiert und promoviert derzeit am Lehrstuhl für Systemsicherheit der Ruhr-Universität Bochum zu Web-Tracking durch Drittanbieter nach Inkrafttreten der DSGVO. Ihre fachlichen Interessen umfassen verschiedene Aspekte der Online-Privatsphäre, wie die technischen Auswirkungen von Datenschutzgesetzen im Web, Datenökonomie und *usable privacy*.

TOBIAS URBAN hat Informatik an der Westfälischen Hochschule studiert und zum Thema Datenschutz im Internet an der Ruhr-Universität Bochum promoviert. Seine Forschungsschwerpunkte liegen in der Analyse des technischen Einflusses von Datenschutzgesetzen im Web und mit menschlichen Aspekten im Datenschutz. Derzeit arbeitet er als Postdoktorand im Institut für Internet-Sicherheit – if(is) und befasst sich mit Themen rund um Vertrauen und Nachhaltigkeit der Digitalisierung.

Literatur

Bundesverband Digitale Wirtschaft (BVDW). 2017. Programmatic Advertising Kompass 2017/2018. https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/programmatic_advertising/kompass_programmatic_advertising_2017_2018.pdf.

Busch, Oliver. 2014. *Realtime Advertising - Digitales Marketing in Echtzeit: Strategien, Konzepte und Perspektiven*. Springer Fachmedien Wiesbaden. http://link.springer.com/book/10.1007%2F978-3-658-05358-1.

Degeling, Martin. 2017. Googles Interessenprofiling. In *Profile. Interdiszplinäre Beiträge*. Digital Cultures. Braunschweig: meson press.

Degeling, Martin, and Jan Nierhoff. 2018. Tracking and Tricking a Profiler: Automated Measuring and Influencing of Bluekai's Interest Profiling. In *Proc. WPES @ CCS*, 1–13. New York, NY, USA: ACM. https://doi.org/10.1145/3267323.3268955.

Degeling, Martin, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2019. We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. In *Proc. NDSS 2019*. Internet Society. https://doi.org/10.14722/ndss.2019.23378.

Edelman, Gilad. 2020. Can Killing Cookies Save Journalism?, *WIRED*. August 5, 2020. https://www.wired.com/story/can-killing-cookies-save-journalism/.

Florian Glatzner. 2018. Erwartungen an die E-Privacy-Verordnung aus Sicht des Verbraucherschutzes, v*orgänge* 57 (221/222): 103-14.

Fouad, Imane, Cristiana Santos, Feras Al Kassar, Nataliia Bielova, and Stefano Calzavara. 2020. On Compliance of Cookie Purposes with the Purpose Specification Principle. In IWPE 2020 - International Workshop on Privacy Engineering, Sep 2020, Genova, Italy. 1-8. https://hal.inria.fr/hal-02567022.

Frik, Alisa, Amelia Haviland, and Alessandro Acquisti. 2020. The Impact of Ad-Blockers on Product Search and Purchase Behavior: A Lab Experiment. In 29th USENIX Security Symposium (USENIX Security 20), 163–179. https://www.usenix.org/conference/usenixsecurity20/presentation/frik.

Härting, Niko. 2020. Neuer Gesetzesentwurf aus dem BMWi: Cookie-Einwilligung per Browsereinstellung und Cookie-Einsatz auf vertraglicher Grundlage. *CR-online.de Blog*, August 3, 2020. https://www.cr-online.de/blog/2020/08/03/neuer-gesetzesentwurf-aus-dem-bmwi-cookie-einwilligung-per-browsereinstellung-und-cookie-einsatz-auf-vertraglicher-grundlage/.

Johnson, Garrett, Scott Shriver, and Samuel Goldberg. 2020. Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR. SSRN Scholarly Paper ID 3477686. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.3477686.

Kleinz, Torsten. 2020. Datenschützer wollen Cookie-Banner prüfen. *Heise.de*. August 20, 2020. https://www.heise.de/news/Datenschuetzer-wollen-Cookie-Banner-pruefen-4874426.html.

Marotta, Veronica, Vibhanshu Abhishek, and Alessandro Acquisti. 2019. Online Tracking and Publishers' Revenues: An Empirical Analysis. In *Proc. WEIS 2019*, 35.

Matte, Célestin, Nataliia Bielova, and Cristiana Santos. 2020. Do Cookie Banners Respect My Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. In *2020 IEEE Symposium on Security and Privacy (SP)*, 791–809. https://doi.org/10.1109/SP40000.2020.00076.

Papadopoulos, Panagiotis, Nicolas Kourtellis, and Evangelos P. Markatos. 2018. Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask. *ArXiv:1805.10505 [Cs]*, May. http://arxiv.org/abs/1805.10505.

Scott, Samuel. 2017. The Day after Tomorrow: When Adblockers and GDPR Kill All Adtech and Martech. *The Drum*. October 17, 2017. https://www.thedrum.com/opinion/2017/10/17/the-day-after-tomorrow-when-ad-blockers-and-gdpr-kill-all-adtech-and-martech.

Soe, Than Htut, Oda Elise Nordberg, Frode Guribye, and Marija Slavkovik. 2020. Circumvention by Design – Dark Patterns in Cookie Consents for Online News Outlets. In *Proc. NordiCHI 2020*. http://arxiv.org/abs/2006.13985.

Solomos, Konstantinos, Panagiotis Ilia, Sotiris Ioannidis, and Nicolas Kourtellis. 2019. Clash of the Trackers: Measuring the Evolution of the Online Tracking Ecosystem. *ArXiv:1907.12860 [Cs]*, July. http://arxiv.org/abs/1907.12860.

Sørensen, Jannick Kirk, and Sokol Kosta. 2019. Before and After GDPR: The Changes in Third Party Presence at Public and Private European Websites. In *WWW '19 Companion Proceedings of the The Web Conference 2019*. Association for Computing Machinery. http://vbn.aau.dk/en/publications/before-and-after-gdpr-the-changes-in-third-party-presence-at-public-and-private-european-websites(350cff41-8ab2-4afa-81d2-9057fdaee76a).html.

Turow, Joseph. 2012. *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*. Yale University Press.

Urban, Tobias, Dennis Tatang, Martin Degeling, Thorsten Holz, and Norbert Pohlmann. 2020. Measuring the Impact of the GDPR on Data Sharing in Ad Networks. In *ASIA CCS '20: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 222–235. http://dx.doi.org/10.1145/3320269.3372194.

Utz, Christine, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)Informed Consent: Studying GDPR Consent Notices in the Field. In *Proc. CCS*, 973–990. CCS '19. New York, NY, USA: ACM. https://doi.org/10.1145/3319535.3354212.

Ward, Chris. 2017. Will GDPR Kill the Third-Party Data Market? *MyCustomer*. September 14, 2017. https://www.mycustomer.com/marketing/data/will-gdpr-kill-the-third-party-data-market.

WhoTracksMe. 2018. GDPR - What Happened? March 9, 2018. https://whotracks.me/blog/gdpr-what-happened.html.

Anmerkungen:

1 S. https://iabeurope.eu/transparency-consent-framework/.
2 S. https://www.enforcementtracker.com/.