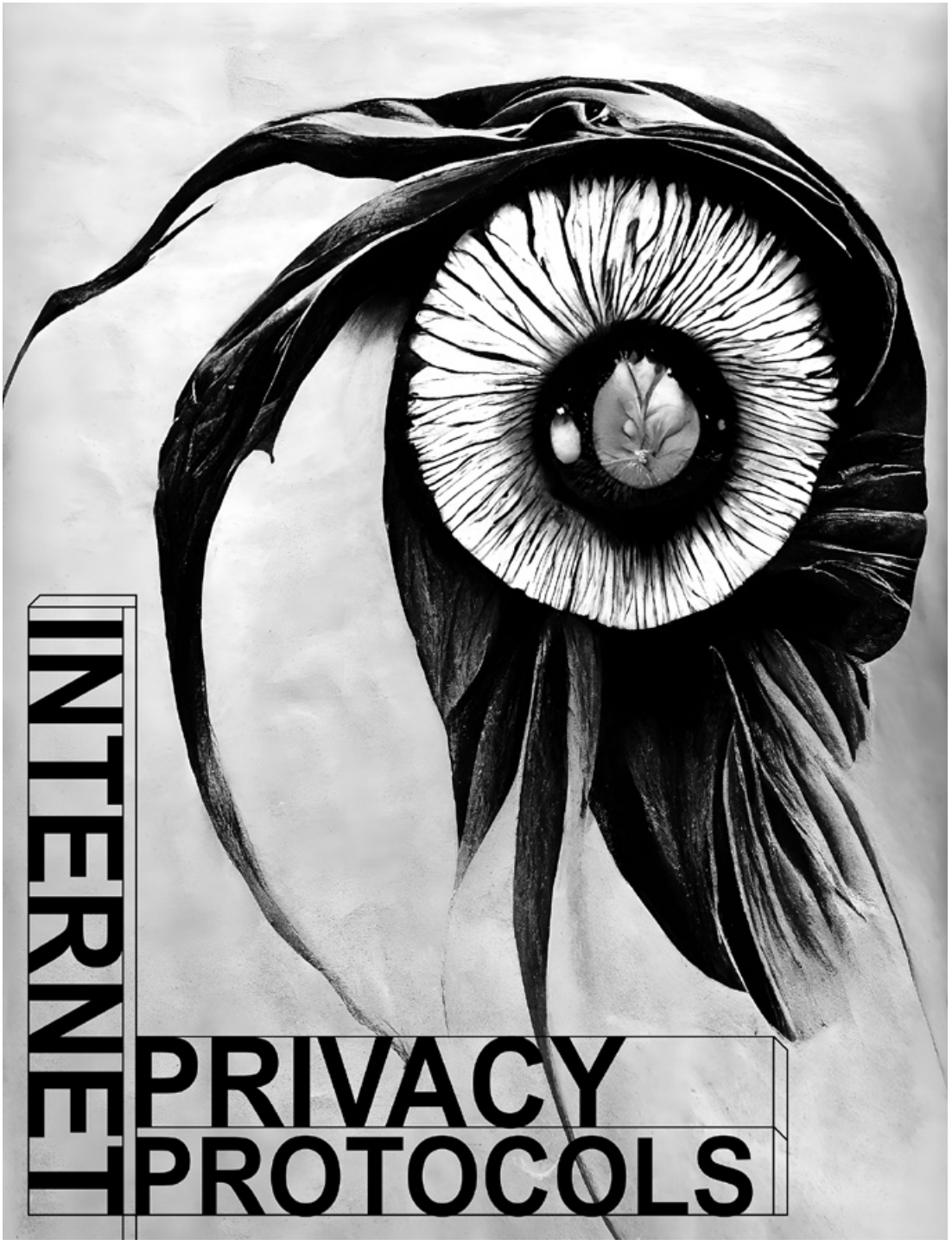

© Soheil Hosseini

MARTIN DEGELING / SOHEIL HUMAN

INTERNET PRIVACY PROTOCOLS

Als das Internet in den 1990er Jahren zunehmend populär wurde, waren viele Hoffnungen und Wünsche an vermeintliche Anonymität geknüpft. Schnell wurde aber klar, dass vollständige Anonymität mit den genutzten Protokollen nicht möglich ist. Selbst ein datenschutzfreundlich konfigurierter Webserver benötigt IP-Adressen, um Websites an die Browser zu verschicken. Mit der Zeit wurde der Bedarf an personenbezogenen Daten über die Nutzer*innen einer Website, insbesondere zum Zweck der Personalisierung und Werbung, immer größer. Offenes und verdecktes Sammeln von Daten auf Websites wurde folglich ein integraler Bestandteil des Webs. Schon früh versuchten verschiedene Initiativen, Protokolle und globale Standards für Datenschutz im Internet zu entwickeln, aber angesichts der offenen Struktur des Webs konnten sich diese Techniken, die von datenorientierten Marktakteur*innen abgelehnt wurden, nicht durchsetzen.

In diesem Artikel werfen wir einen Blick auf die Geschichte der Internet-Datenschutzprotokolle, die in den letzten Jahrzehnten entstanden sind, und zeigen, wie sie (bisher) nicht in der Lage gewesen sind, die datengetriebenen Praktiken der Webdienstanbieter*innen zu verändern. Entlang Lawrence Lessigs vier «modalities of regulation» (*code*, *law*, *market* und *norms*)[1] werden wir die selbst-regulatorischen, technischen Initiativen wie die Platform for Privacy Preferences Project (P3P) und Do Not Track (DNT) der frühen 2000er Jahre in einen Zusammenhang stellen mit neueren gesetzlichen Bestimmungen wie der Datenschutzgrundverordnung (DSGVO) und dem California Consumer Privacy Act (CCPA), die zwar keine spezifischen Protokolle vorsehen, aber die Debatte um neue Protokolle wie Federated Learning of Cohorts (FLoC), Global Privacy Control (GPC) oder Advanced Data Protection Control (ADPC) entfacht haben. Allen Ansätzen gemein ist ein Verständnis von Privatheit, das sich auf Transparenz und individuelle Einwilligung konzentriert. Gemeinsam ist ihnen auch, dass sie bisher von der breiten Masse der Unternehmen des Überwachungskapitalismus[2] ignoriert oder ausgehebelt werden. Nach fast

1 Lawrence Lessig: *Code and Other Laws of Cyberspace*, New York, 1999, 121–132.

2 Shoshana Zuboff: *Das Zeitalter des Überwachungskapitalismus*, übers. v. Bernhard Schmid, Frankfurt / M., New York 2018.

30 Jahren Debatte um Internet-Privacy-Protokolle zeichnet sich ab, dass erst seit der verstärkten Regulierung durch die DSGVO und den CCPA und der beginnenden Durchsetzung dieser Vorgaben eine Entwicklung eingesetzt hat, die eine Zusammenführung der Erwartungen von Nutzer*innen und Marktgeschehen möglich erscheinen lassen. Der Beitrag schließt mit einer Auflistung von Gegensätzen in den Protokollen, die aktuell diskutiert werden, und fragt, ob die aktuell diskutierten technischen Lösungen einen Ausgleich zwischen den verschiedenen Modalitäten der Regulierung leisten können.

Einführung: Datenschutz und das Internet

Die Sorge um Privatsphäre war von Beginn an Teil der Debatten um das Internet. Im April 1995, nicht lange nachdem grafische Browser 1993 dazu beigetragen hatten, das ‹Surfen› im Internet populär zu machen, veranstaltete die amerikanische Federal Trade Commission (FTC), die für den Schutz der Verbraucher*innenrechte zuständig ist, ihren ersten Workshop zum Thema Datenschutz im Internet. Damals ging es v. a. um Websites, die die Nutzer*innen aufforderten, personenbezogene Daten direkt an die Websites zu übermitteln, ohne Informationen darüber bereitzustellen, wie Daten verwendet oder weitergegeben werden würden.

Während sich die FTC in erster Linie für Transparenz einsetzte, begannen Websites ihr Geschäft durch personalisierte Online-Werbung zu finanzieren, wodurch ein weiteres Datenschutzproblem entstand, das an Bedeutung seitdem zugenommen hat. Zwar wurde die erste Online-Werbung im Jahr 1994 wie ein allgemeiner Werbeplatz in einer Offline-Zeitschrift verkauft, wobei drei Monate lang dieselbe Anzeige zu einem Festpreis gezeigt wurde – ohne dass persönliche Daten benötigt wurden. Doch schon bald darauf, Anfang 1995, tauchten die ersten Werbemarktplätze auf, die Werbung individualisierten. Bereits Ende 1995 wurde DoubleClick gegründet, das erste Unternehmen, das heute zu Google gehört und das Cookies zur Verfolgung und Profilierung von Nutzer*innen auf verschiedenen Websites einsetzte.[3]

Information und Einwilligung

Eine der wesentlichen Normen zum Schutz der Privatsphäre ab den 1990er Jahren bis heute basiert häufig auf dem *notice-and-choice*-Prinzip. Bei der FTC sind dieses und weitere Grundsätze in den *Fair Information Principles* zusammengefasst, die in den USA 1973 entworfen wurden. In Deutschland wurden zur selben Zeit ähnliche Grundsätze formuliert. In einem 1971 erstellten Gutachten für das Bundesinnenministerium, das die Grundlage für viele Datenschutzgesetze schuf, sind Information und Einwilligung ebenfalls zentrale Bestandteile.[4] Dabei bezieht sich das Prinzip in beiden Fällen auf den Austausch von Daten zwischen einer Einzelperson und einer privaten Institution – die

3 Vgl. Martin Kihn: Paleo Pellet: How DoubleClick worked, in: *Paleo Ad Tech – The Secret History of Advertising on the Internet*, Audio-Aufzeichnung, 9.11.2021, paleoadtech.com/2021/11/09/paleo-pellet-how-doubleclick-worked (12.10.2022).

4 Vgl. Wilhelm Steinmüller u. a.: *Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern*, Drucksache VI/3826, Anlage 1, Deutscher Bundestag, 7.9.1972, *dserver.bundestag.de/btd/06/038/0603826.pdf* (16.12.2022).

Datenverarbeitung durch staatliche Stellen war und ist meist separat geregelt. Der Begriff ‹Information› bezieht sich auf die Notwendigkeit, die Person, deren Daten gesammelt und verarbeitet werden, über die Einzelheiten der Verarbeitung zu informieren. Wer darf welche Daten für welche Zwecke verwenden? Das offensichtlichste Beispiel für einen Datenschutzhinweis ist eine Datenschutzerklärung. Auf der Grundlage dieser Informationen sollte der*die Einzelne die ‹Wahl› haben, diesen Praktiken zuzustimmen oder eine*n andere*n Akteur*in auf dem Markt zu suchen. Das *notice-and-choice*-Prinzip geht dabei von einem Idealzustand der Transaktion von Daten zwischen rationalen Akteur*innen aus. In der Praxis sind die Probleme der Benutzer*innenfreundlichkeit von Datenschutzerklärungen und Cookie-Bannern sowie die fehlenden Alternativen zu den großen Plattformen hinlänglich bekannt. Es fehlt aber auch eine Berücksichtigung jenseits eines rein individualistischen Ansatzes für den Datenschutz, der die relationalen Aspekte von Informationen berücksichtigt, wenn Daten nicht nur eine Person, sondern Gruppen betreffen. Dass Daten als tauschbare Ware behandelt werden, verkennt zudem die Tatsache, dass sie vervielfältigt, in andere Zusammenhänge gestellt und zu einem anderen Zeitpunkt auf neue Art verarbeitet werden können, die in dem Moment, in dem wir auf «Ich akzeptiere» geklickt haben, nicht vorstellbar sind. Untersuchungen zu sozialen Netzwerken und Online-Werbung haben gezeigt, dass nur wenige Menschen mitbedenken, wie ihre Daten verwendet werden oder was aus ihnen abgeleitet werden kann.[5]

«P3P and history»

Wichtige technische Protokolle zur Verbesserung des Datenschutzes im Internet – also Regulierung durch Code – gehen zurück auf von der FTC organisierte Workshops. Die FTC veranstaltete ab 1995 Workshops und Anhörungen zum Thema Verbraucher*innen-Datenschutz. Aus diesen Diskussionen gingen frühe Protokolle wie P3P (Platform for Privacy Preferences Project) hervor, die in den Arbeitsgruppen des World Wide Web Consortium (W3C) standardisiert wurden. Das W3C definiert bis heute die höheren Protokolle wie HTTP,[6] auf denen das Internet aufbaut, und HTML, das bestimmt, wie Browser Websites darstellen.

P3P

Die Entwicklung von P3P vollzieht Lorrie Cranor in einem 2002 erschienenen Buch nach, das sich an Entwickler*innen richtet.[7] Danach begannen die Diskussionen 1996 mit einem «Consumer Privacy On the Global Information Infrastructure» betitelten FTC-Workshop.[8] Bei diesem Workshop schlugen Forscher*innen vor, die bereits ein Jahr zuvor vom W3C standardisierte Platform for Internet Content Selection (PICS) zu erweitern. PICS war Teil der frühen Bemühungen um das semantische Web, die darauf abzielten, (Web-)

5 Vgl. Idris Adjerid, Alessandro Acquisti, George Loewenstein: Choice Architecture, Framing, and Cascaded Privacy Choices, in: *Management Science*, Bd. 65, Nr. 5, 2019, 2267–2290, doi.org/10.1287/mnsc.2018.3028.

6 Tieferliegende Protokolle wie TCP/IP werden von der Internet Engineering Task Force entwickelt.

7 Lorrie Faith Cranor: *Web Privacy with P3P*, Sebastopol 2002.

8 Ankündigung des Workshops auf der Website der Federal Trade Commission: ftc.gov/news-events/events/1996/06/consumer-privacy-global-information-infrastructure (31.1.2023).

Inhalte in einem vordefinierten Schema zu beschreiben, um deren Inhalt und Kontext automatisch auswertbar zu machen. PICS wurde hauptsächlich zur Kategorisierung und Bewertung von Websites im Hinblick auf ihre Eignung für Kinder verwendet. Zu diesem Zweck konnten Browser so konfiguriert werden, dass sie Websites mit bestimmten Bewertungen blockierten.

Paul Resnick, wie auch Cranor damals bei AT & T in der Abteilung ‹Public Policy Research› beschäftigt, führte hierzu auf dem Workshop aus:

> [D]ie große Idee hier ist, dass, wenn wir den Hinweis in ein Standardformat packen und den Leuten erlauben, ihre Präferenzen auszudrücken, die Software den Vergleich automatisch durchführen kann und dass zumindest manchmal der Hinweis und die Auswahl im Hintergrund geschehen, anstatt immer eine Last zu sein.[9]

Er beschrieb aber auch die Probleme dieses Ansatzes, die er in der Notwendigkeit eines standardisierten Vokabulars und der Selbstregulierung durch die Web-Industrie sah. Alle semantischen Beschreibungsbemühungen sind darauf angewiesen, dass der*die Eigentümer*in der Website Angaben macht, die den definierten Standards entsprechen und natürlich den Inhalt der Website wahrheitsgemäß wiedergeben. Ein Jahr später wurde ein erster Prototyp eines Protokolls vorgestellt.[10] Im Laufe der nächsten zwei Jahre wurde eine Spezifikation entwickelt, die dann aufgrund der Bedenken von Wirtschaftsvertreter*innen stark vereinfacht wurde. Unter anderem wurden Funktionen entfernt, die eine automatische Aushandlung von Datenfreigaben ermöglichen sollten. Die Diskussion um P3P wurde 1997 in eine technische Architekturgruppe (TAG) des W3C verlagert und eine erste gültige Fassung des Standards erschien 2002.[11]

Zu diesem Zeitpunkt ist auch die erste Stimme aus der europäischen Politik dokumentiert.[12] Nach Cranor gab die Europäische Kommission eine Stellungnahme zu P3P ab, die Punkte enthielt, welche auch 20 Jahre später in der Datenschutz-Grundverordnung wiederzufinden sind: Datenschutzvorschriften müssen rechtlich abgesichert werden, um durchgesetzt werden zu können. In der Stellungnahme wurde auch eine klare Definition von Mindeststandards gefordert.

Um P3P zu unterstützen, müssen Websites mehrere Dokumente erstellen und so referenzieren, dass ein Browser sie automatisch abrufen kann. Zuerst braucht es eine P3P-Policy, die einer formalisierten Datenschutzerklärung entspricht und in einer XML-basierten Struktur geschrieben ist. Hierfür wurde in der Spezifikation eine Terminologie bereitgestellt. Zusätzlich zu der vollständigen P3P-Policy erlaubte die Spezifikation, eine ‹kompakte Richtlinie› als HTTP-Header zu senden. HTTP-Header sind rein textbasierte technische Informationen, die bei jedem Aufruf einer Website mitgesendet werden und keine zusätzlichen Aufrufe erfordern. Die kompakte Policy sollte sich nur auf Cookies beziehen. Der Header enthielt eine Reihe von dreistelligen Abkürzungen, die, wie in der allgemeinen Richtlinie beschrieben, als spezifische Kombinationen von Elementen interpretiert werden konnten. So bedeutet beispielsweise die

9 Paul Resnick, zit. in Federal Trade Commission: Federal Trade Commission: Public Workshop on Consumer Privacy on the Global Information Infrastructure, 4.6.1996, 4.6.1999, hier 87, *ftc.gov/sites/default/files/documents/public_events/consumer-privacy-global-information-infrastructure/pw960604.pdf* (28.10.2022) (eigene Übers.).

10 Der ursprüngliche Prototyp ist immer noch online verfügbar unter *w3.org/Talks/970612-ftc/ftc-sub.html* (28.10.2022).

11 Die Version 1.0 der Spezifikation ist abrufbar unter *w3.org/TR/P3P/* (12.12.2022).

12 Vgl. Cranor: *Web Privacy with P3P*, 54.

Header-Information «OTI IVA OUR», dass eine beliebige Kennung (OTI) für individuelle Analysen (IVA) verwendet und über einen vom Unternehmen bestimmten Zeitraum gespeichert wird (OUR).

2008 verfügten etwa 21 Prozent der 5000 meistbesuchten Websites (in den USA) über eine P3P-Policy.[13] Obwohl die meisten Browser P3P nicht umsetzten und beispielsweise Mozilla die Unterstützung bereits 2007 einstellte, wurde P3P von Microsofts Internet Explorer – in den 2000er Jahren der Browser mit dem größten Marktanteil – weiterhin unterstützt. Der selbstregulierende Ansatz hat sich jedoch nicht nur in Bezug auf seine Verbreitung nicht bewährt. In einer Studie von 2010 stellten die Autor*innen fest, dass ein Drittel der 33.000 untersuchten Websites P3P nicht korrekt umsetzten.[14] Während dies einerseits auf die Komplexität von P3P zurückgeführt wurde, fanden die Autor*innen auch 2700 Websites, die dieselbe ungültige Richtlinie verwendeten. Der Ursprung dieser fehlerhaften Beschreibung der Datenschutzpraxis lag ironischerweise bei Microsoft. Es gab ein bekanntes Problem in der Kombination der kompakten Policys und der Verwendung von Frames beim Internet Explorer, für die Microsoft selbst in einem Blogpost die Verwendung einer speziellen, aber ungültigen kompakten Policy empfahl.[15]

Do Not Track

Während sich abzeichnete, dass P3P sich nicht durchsetzen würde, entstand ab 2007 mit Do Not Track ein Standard, der technisch wesentlich weniger komplex war und ebenfalls ausschließlich auf einem HTTP-Header beruhte. Während P3P davon ausging, dass Websites ihren Besucher*innen etwas mitzuteilen hätten, geht es bei DNT um eine Informationsübermittlung in die andere Richtung: Das Senden der binären DNT:1-Header-Information durch den Browser soll Webservern signalisieren, dass der*die Absender*in nicht verfolgt werden möchte. Firefox unterstützte DNT ab Februar 2012, andere folgten. Durch die Umsetzung im Browser war es wesentlich einfacher, die Marktdurchdringung zu erreichen.

DNT wurde 2007 von mehreren Datenschutzgruppen, darunter die Electronic Frontier Foundation (EFF) und das Center for Democracy and Technology (CDT), als eine Kampagne initiiert, in deren Rahmen die FTC dazu aufgefordert wurde, eine Do-Not-Track-Liste zu erstellen.[16] Der Vorschlag sah vor, dass sich jedes Online-Marketingunternehmen bei der FTC registrieren müsste, um u. a. die von ihm genutzten Internetdomains anzugeben. Die FTC sollte diese Liste dann an Browser-Anbieter*innen weitergeben können, damit diese, ähnlich wie Werbeblocker-Add-ons, dann jene Domains blockieren könnten. Der Unterschied zu Werbeblockern bestand dabei darin, dass diese sich auf eine manuell kuratierte Liste von Domains stützten, die von Freiwilligen gepflegt wurden (und bis heute werden),[17] statt von einem von einer Regierungsbehörde geführten Register. Drei Jahre später erwähnte

13 Vgl. Lorrie Faith Cranor u. a.: P3P deployment on websites, in: *Electronic Commerce Research and Applications*, Bd. 7, Nr. 3, 2008, 274–293, hier 274, doi.org/10.1016/j.elerap.2008.04.003.

14 Vgl. Pedro Giovanni Leon u. a.: Token attempt: the misrepresentation of website privacy policies through the misuse of p3p compact policy tokens, in: *WPES '10: Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, 4.10.2010, 93–104, hier 93, doi.org/10.1145/1866919.1866932.

15 Vgl. ebd., 98.

16 Vgl. Ryan Singel: Privacy Groups Call For Do-Not-Track-Me List to Rein in Online Ad Firms, in: *Wired*, 31.10.2007, wired.com/2007/10/privacy-groups-2 (27.9.2022).

17 Vgl. Website easylist.to (28.10.2022); hier stehen verschiedene Blocklisten zur Verfügung, die ganze Domains oder Teile von Websites im Browser blockieren, um z. B. Werbeeinblendungen zu verhindern.

der Vorsitzende der FTC bei einer Anhörung vor dem US-Senat zum Thema Online-Datenschutz eine Do-Not-Track-Liste.

Beim W3C waren beide Ideen, sowohl die der Filterliste als auch die eines separaten Headers, Teil einer ersten Einreichung von Microsoft im Jahr 2011;[18] der erste technische Spezifikationsentwurf konzentrierte sich dann allerdings nur noch auf den Header.[19] Die Hauptaktivität im Zusammenhang mit der Standardisierung fand zwischen 2011 und 2014 statt, als sieben verschiedene Spezifikationen veröffentlicht und fast 10.000 E-Mails über die Projekt-Mailingliste ausgetauscht wurden.[20] Das Einfügen eines HTTP-Headers war selbst keine besondere Schwierigkeit. Länger zogen sich die Debatten darum, was das eine Bit an Informationen für Folgen bei denen haben sollte, die es empfangen: Es ging um Fragen des Trackings, darum, ab wann eine Re-Identifizierung als Tracking gelten sollte, wer sich durch DNT angesprochen fühlen sollte und welche konkreten Maßnahmen ergriffen werden sollten. Während diese Diskussionen fortgeführt wurden, erreichte der Standardisierungsprozess insgesamt nur einen ‹Kandidatenstatus›, bevor die Entwicklung 2019 endgültig eingestellt wurde.

Der erste Rückschlag für DNT war 2012 die Ankündigung von Microsoft, den DNT-Header standardmäßig einzuschalten. Dieser Schritt wurde schnell von Online-Werbeunternehmen angegriffen, die im Gegenzug ankündigten, DNT zu ignorieren. Im Dezember 2014 kritisierte ein Artikel in der *New York Times*, dass die damals aktuelle Version der Spezifikation v. a. kleinen Tracking-Unternehmen schaden würde, da Google und Facebook nach den Definitionen als Unternehmen mit direkten Verbindungen zu den Kund*innen das DNT-Attribut ignorieren könnten.[21] Grund für das Scheitern von DNT sei, dass die Spezifikation des Protokolls von der FTC an eine industriedominierte Gruppe beim W3C übergeben worden sei.

Größere Studien zur Umsetzung von DNT sind rar, da nicht automatisiert überprüft werden kann, wie die Empfänger*innen-Seite DNT umsetzt. Ende 2018 erwähnten nur 14 der 32 meistgenutzten Werbenetzwerke DNT in ihrer Datenschutzerklärung.[22] Nur fünf gaben an, DNT zu unterstützen und das Tracking einzustellen, sollte der Browser den entsprechenden HTTP-Header senden.

AdChoices

Exemplarisch für die Regulierung durch den *Markt* ist das AdChoices-Programm, das 1999 von der Digital Advertising Alliance (DAA), einer Interessengruppe der Online-Werbe-Industrie, als Reaktion auf die Kritik am Online-Tracking gegründet wurde. Die DAA hat zwar nie einen technischen Standard oder ein Protokoll vorgeschlagen, aber an den oben genannten mitgewirkt. Bis heute findet sich in Online-Anzeigen ein kleines blaues AdChoices-Dreieck. Auf der verlinkten Website können Nutzer*innen manuell das Tracking von 125 Unternehmen deaktivieren. Anstelle eines einheitlichen Protokolls

18 Vgl. Andy Zeigler, Adrian Bateman, Eliot Graff: Web Tracking Protection, *W3C*, 24.2.2011, *w3.org/Submission/web-tracking-protection/* (10.10.2022).

19 Vgl. Roy T. Fielding: Tracking Preference Expression (DNT), *W3C*, 14.11.2011, *w3.org/TR/2011/WD-tracking-dnt-20111114* (10.10.2022).

20 Archiv verfügbar auf der W3C-Website, *lists.w3.org/Archives/Public/public-tracking* (28.10.2022).

21 Vgl. Fred B. Campbell: The Slow Death of ‹Do Not Track›, in: *New York Times*, 26.12.2014, *nytimes.com/2014/12/27/opinion/the-slow-death-of-do-not-track.html* (31.10.2022).

22 Vgl. Tobias Urban u. a.: A Study on Subject Data Access in Online Advertising After the GDPR, in: Cristina Pérez-Solà u. a. (Hg.): *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2019 International Workshops, DPM 2019 and CBT 2019, Luxembourg, September 26–27, 2019, Proceedings*, Cham 2019, 61–79, hier 79.

speichert der Dienst Opt-out-Cookies für jeden einzelnen Dienst im Browser. Der Nachteil dieses Vorgehens ist, dass mit dem Entfernen von Cookies aus dem Browser auch die Opt-outs gelöscht werden, zudem wird die tatsächliche Zahl der Unternehmen, die Tracking zu Werbezwecken einsetzen, wesentlich höher geschätzt.[23]

Europäische Datenschutzgesetze als Intervention

Die oben beschriebenen Protokolle, die dazu dienen, Datenschutz im Internet zu verbessern und insbesondere Tracking einzudämmen, wurden ausschließlich von US-Institutionen vorangetrieben und waren auf Selbstregulierung ausgerichtet. Eine gesetzliche Regulierung (*law* im Sinne Lessigs) bestand v. a. in der EU, wo die 2002 in Kraft getretene Datenschutzrichtlinie für elektronische Kommunikation erste Standards setzte (2009 wurde die Richtlinie novelliert). Sie enthält klare Aussagen zur Verwendung personenbezogener Daten und insbesondere von Cookies. In technologieneutraler, jedoch nicht geschlechtsneutraler Sprache verlangt sie, «dass die Speicherung von Informationen […] im Endgerät eines Teilnehmers oder Nutzers […] nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen […] seine Einwilligung gegeben hat».[24] Für Cookies bedeutet diese Einwilligung ein aktives Opt-in statt der vom DNT favorisierten Opt-out-Variante. Dieses Opt-in soll mit Informationen einhergehen, die es Nutzer*innen ermöglichen, eine bewusste Entscheidung zu treffen. Die europäische Rechtsarchitektur sieht vor, dass Richtlinien mit einer Frist von vier Jahren in nationales Recht umgesetzt werden müssen. Eine Studie aus dem Jahr 2017 hat jedoch gezeigt, dass nur knapp die Hälfte der Websites die seit 2013 geltenden Vorschriften befolgen.[25] So konstatieren die Autor*innen für die Kategorie ‹Nachrichten und Medien›, dass 89 Prozent der Websites ohne Zustimmung ein Nutzer*innenprofil erstellen.

Im Jahr 2018 legte die Datenschutzgrundverordnung (DSGVO) strengere Standards für die Verarbeitung personenbezogener Daten durch Online- und Offline-Dienste in der EU fest. Die DSGVO, die im Unterschied zur ePrivacy-Richtlinie ohne Umsetzung in nationales Recht und dadurch schneller in Kraft treten konnte, enthält keine wesentlichen Änderungen in den Regularien, sie setzt weiter auf Information und Einwilligung in Form von Opt-in, bietet aber die Möglichkeit, Unternehmen bei Datenschutzverstößen mit hohen Strafen von bis zu 4 Prozent des gesamten weltweiten Jahresumsatzes zu belegen. Die Auswirkungen auf die Internetindustrie waren gemischt: Die DSGVO führte dazu, dass mehr Websites Datenschutzerklärungen und Cookie-Banner enthielten; den Einsatz von Cookies hat sie allerdings zunächst nicht beeinträchtigt.[26] Weitere Studien zeigen, dass die Weitergabe von Tracking-Daten innerhalb von Werbenetzwerken an weitere Unternehmen deutlich zurückgegangen ist.[27]

23 Die Website *WhoTracksMe*, die kontinuierlich Websites auf Tracker untersucht und diese klassifiziert, listet 928 solcher Unternehmen, vgl. *whotracks.me/trackers.html* (12.12.2022).

24 Art. 5, Abs. 3 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates, 25.11.2009, *data.europa.eu/eli/dir/2009/136/oj/deu* (31.10.2022).

25 Vgl. Martino Trevisan u. a.: 4 Years of EU Cookie Law: Results and Lessons Learned, in: *Proceedings on Privacy Enhancing Technologies*, Bd. 2019, Nr. 2, 2019, 126–145, *doi.org/10.2478/popets-2019-0023*.

26 Vgl. Martin Degeling, Christine Utz, Tobias Urban: Effekte der DSGVO auf Websites und die Entwicklung der ePrivacy-Verordnung, in: *vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik*, Bd. 59 (3/4), Nr. 231/232, 2020, 77–86.

27 Vgl. Tobias Urban u. a.: Measuring the Impact of the GDPR on Data Sharing, in: *ASIA CCS '20: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 5.10.2020, 222–235, *doi.org/10.1145/3320269.3372194*.

Da es sich bei der DSGVO um ein Gesetz und nicht um einen technischen Standard handelt, sind genaue Protokolle für die Einwilligung nicht definiert. Mehrere Studien weisen darauf hin, dass sich seit 2018 Praktiken zum Einholen einer Einwilligung entwickelt haben, welche die gesetzlichen Vorgaben möglichst weit auslegen und nicht selten überschritten haben. Kretschmer u. a. halten in einer Übersichtsstudie zusammenfassend fest, dass seit dem Inkrafttreten der GDPR «Online-Dienste ihren Nutzern immer häufiger Möglichkeiten bieten, der Datenverarbeitung zu widersprechen, aber regelmäßig den Zugang durch unnötig komplexe und manchmal unzulässige Schnittstellengestaltung erschweren» sowie dass diese Situation im Widerspruch zu den Wünschen steht, «die die Nutzer*innen sowohl mündlich als auch durch ihr Handeln zum Ausdruck gebracht haben».[28]

Consent-Management-Plattformen und das Ende von Cookies

Heutzutage nutzen viele Websites, die, um Strafen zu vermeiden, an der Einhaltung der gesetzlichen Vorgaben interessiert sind, sogenannte Consent-Management-Plattformen (CMP), die automatisierte Lösungen für die Einbettung von Cookie-Bannern in Websites anbieten. Einerseits stellen CMPs den Entwickler*innen technische Mittel zur Verfügung, um externe Dienste zu identifizieren, die in einer Website integriert sind und gleichzeitig Cookies setzen (Werbung, aber auch etwa Video-Einbettungen), und können dabei helfen, diese zu deaktivieren, solange ein*e Nutzer*in keine ausdrückliche Zustimmung erteilt hat. Andererseits unterstützen CMP-Anbieter*innen Website-Betreiber*innen bei der *consent optimization*, womit im Marketingjargon Praktiken bezeichnet werden, die darauf abzielen, die Opt-in-Rate zu erhöhen. Hierbei wird die Einwilligung zu einer notwendigen Marketing-Kennzahl, bei der durch Tests verschiedener Gestaltungen und der schriftlichen Erläuterung versucht wird, eine möglichst hohe Zustimmungsrate zu erhalten. In einem Whitepaper stellt eine der führenden CMP-Anbieterinnen in Europa fest: «Langfristig werden die Zustimmung und das damit verbundene Vertrauen der Nutzer die neue Währung im Marketing werden.»[29] Die Firma empfiehlt, zunächst die Zahl der Nutzer*innen zu erhöhen, die mit einem Cookie-Banner interagieren, da die meisten versuchen würden, diesen zu ignorieren und – wenn sie dazu gezwungen seien – ohnehin auf «Akzeptieren» klicken würden.

CMP-Anbieter*innen befinden sich in einer eigentlich unmöglichen Rolle. Ihr Geschäftsmodell basiert auf dem Versprechen an Website-Betreiber*innen, die Komplexität der DSGVO-Konformität übernehmen zu können, während sie gleichzeitig versuchen müssen, die Einschnitte, z. B. bei Werbeeinnahmen, so gering wie möglich zu halten. Dies funktioniert aber nur, wenn die Nutzer*innen überzeugt werden können, auf ihren Datenschutz zu verzichten. Eine Analyse fünf solcher CMP-Anbieter*innen durch Toth u. a. konnte auch

28 Michael Kretschmer, Jan Pennekamp, Klaus Wehrle: Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web, in: *ACM Trans. Web*, Bd. 15, Nr. 4, Artikel 20, Juni 2021, 1–42, hier 1 (eigene Übers.).

29 Usercentrics: *Optimising the Opt-in Rate A new discipline in online marketing*, Juni 2020, usercentrics.com/wp-content/uploads/2020/06/Whitepaper-_-Opt-in-Optimization.pdf (19.10.2022) (eigene Übers.).

zeigen, dass die angebotenen Standardkonfigurationen von Cookie-Bannern nicht den aktuellen rechtlichen Anforderungen genügen[30] und dass die CMP-Anbieter*innen selbst von sogenannten *dark patterns* Gebrauch machen, die Website-Betreiber*innen dazu bringen sollen, kostenpflichtige Zusatzangebote zu buchen.[31]

Andere sind bereits einen Schritt weiter gegangen und haben die Einwilligung selbst zu einem handelbaren Gut transformiert. Ein verbreitetes Instrument zum Einwilligungsmanagement ist das Transparency and Consent Framework (TCF) des Interactive Advertising Bureau (IAB). Die Mitgliedschaft in diesem Netzwerk von Marketingfirmen, die Zustimmungen einzelner Nutzer*innen untereinander weitergeben, kostet 1500 Euro pro Jahr. Das zugehörige Protokoll legt fest, wie Websites Einwilligungen so gestalten können, dass sie nicht nur für die Website gelten, auf der sie abgefragt werden, sondern zentral für einen Dienst eingeholt und ausgetauscht werden können. Gegenüber denjenigen, deren Daten gesammelt werden, wird das TCF als eine Möglichkeit dargestellt, die Anzahl der Cookie-Banner zu begrenzen, da eine Einwilligung zwischen den Websites ausgetauscht wird, sodass die Nutzer*innen nicht jeweils individuell befragt werden müssen. Aber für Websites und Werbetreibende ist es eine Möglichkeit, auf eine Datenbank zurückzugreifen, zu der auch Websites beitragen, die sich nicht unbedingt an die Regeln der informierten Einwilligung halten.[32] Im Februar 2022 verhängte die belgische Datenschutzbehörde daher eine Geldstrafe gegen das IAB; die endgültige gerichtliche Entscheidung darüber, ob diese Praxis mit der DSGVO vereinbar ist, steht noch aus.

Parallel zur rechtlichen Debatte und zu den technologischen Entwicklungen, die die Einhaltung der Vorschriften gewährleisten sollen, versucht Google, wie 20 Jahre zuvor Microsoft, seine Position als Anbieter*in des aktuell meist verwendeten Browsers zu nutzen, um eine Änderung der DSGVO durchzusetzen. 2019 kündigte Google an, die Unterstützung für Cookies von Drittanbieter*innen in Google Chrome bis 2022 zu entfernen. Auf die Ankündigung folgten mehrere technische Vorschläge, die die gleichen Vorteile der Profilerstellung auf Basis anderer Technologien bieten sollten, wobei die Datenerfassung hauptsächlich auf die Google-Plattform verlagert wurde. Im Frühjahr 2021 wurde etwa Federated Learning of Cohorts (FLoC) im Google Browser erstmals getestet. Hierbei werden Nutzer*innen auf Basis ihres Surfverhaltens gruppiert und Interessen-Kohorten zugeordnet, die dann von Websites abgerufen und bei der Personalisierung von Werbung berücksichtigt werden können. Bereits wenige Wochen nachdem der Test öffentlich bekannt gemacht wurde, hatten alle weiteren Browser-Hersteller*innen der Technik bereits eine Absage erteilt. Wenige Monate später zog Google den Test und den gesamten Vorschlag zurück und stellte als Ersatz die Topics API vor, die eine feste Liste von Interessen vorgibt statt eine beliebigen Zuordnung vorzunehmen. Die grundsätzliche Kritik blieb allerdings gleich: Erstens würde die Implementierung im

30 Vgl. Michael Toth, Nataliia Bielova, Vincent Roca: On dark patterns and manipulation of website publishers by CMPs, in: *Proceedings on Privacy Enhancing Technologies*, Nr. 3, 2022, 478–497, petsymposium.org/popets/2022/popets-2022-0082.pdf (16.12.2022).

31 *Dark Patterns* sind Praktiken der Gestaltung von Websites, die darauf abzielen, Nutzer*innen zu einem bestimmten Verhalten zu drängen, z. B. das Akzeptieren von Cookies oder auch das möglichst schnelle Abschließen eines Kaufs auf Shopping-Websites. Für eine Liste von *dark patterns* vgl. Arnuesh Mathur u. a.: Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites, in: *Proceedings of the ACM on Human-Computer Interaction*, Bd. 3, Nr. CSCW, November 2019, doi.org/10.1145/3359183.

32 Vgl. Célestin Matte, Nataliia Bielova, Cristiana Santos: 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 (S&P)*, 2020, 791–809, doi.org/10.48550/arXiv.1911.09964.

Browser zu einer Monopolstellung durch Google führen, die es zu verhindern gelte.[33] Zweitens seien Googles Vorschläge techno-zentrisch und könnten den Widerspruch, dass das Unternehmen einerseits mehr Datenschutz verspreche und andererseits wesentlicher Profiteur im Überwachungskapitalismus sei, nicht lösen.[34] Eine nachträgliche Analyse von FLoC konnte dann auch zeigen, dass der versprochene Datenschutzgewinn durch Anonymisierungstechniken bei der Berechnung und Verarbeitung der Daten im Browser durch die Eindeutigkeit der Profile ausgehebelt wird.[35] Aufgrund der mangelnden Zustimmung zu den neuen Techniken und fehlenden Alternativen hat Google die Pläne für das Ende von Cookies zuletzt auf 2024 verschoben.[36]

Was folgt: GPC und ADPC

Nach dem Ende von P3P und DNT geriet die Debatte über öffentlich entwickelte Standards eine Zeit lang ins Stocken. Aktuelle Initiativen auf der Ebene von *code* orientieren sich nun direkt an den regulatorischen Vorgaben (*law*), insbesondere der DSGVO und dem 2019 in Kraft getretenen California Consumer Privacy Act (CCPA), der v. a. dadurch Wirkung entfaltet, dass er für alle in Kalifornien und im Silicon Valley ansässigen Unternehmen Anwendung findet.

Einer der wichtigsten Unterschiede von Datenschutzprotokollen, die auf der Grundlage des CCPA oder der DSGVO entwickelt worden sind, besteht darin, ob sie dem Opt-in- oder den Opt-out-Ansatz folgen. Während zur Kommunikation eines globalen Opt-out ein binäres Attribut ausreichen könnte, sind zur Kommunikation von Opt-in-Informationen und Einwilligungen komplexere Mechanismen erforderlich. Auf der Grundlage des CCPA wurde dem W3C mit Global Privacy Control (GPC) ein Nachfolger für DNT vorgeschlagen, und gleichzeitig wird mit Advanced Data Protection Control (ADPC) ein auf DSGVO-Überlegungen basierendes Protokoll entwickelt.[37]

GPC

Nach dem Scheitern von DNT wurde die Entwicklung neuer Opt-out-Datenschutzprotokolle für eine Weile ausgesetzt. Die Durchsetzung des CCPA in Kalifornien lieferte jedoch eine neue gesetzgeberische Motivation und Unterstützung. Gemäß dem CCPA haben Nutzer*innen das Recht, den Verkauf oder die Weitergabe ihrer persönlichen Daten abzulehnen, und Unternehmen müssen es ihnen ermöglichen, dieses Recht auszuüben. GPC wurde entwickelt, um diese CCPA-Anforderung (und die des DSGVO-Rechts auf *Widerspruch*) zu erfüllen, aber nicht weitergehende rechtliche Vorgaben der DSGVO wie die der informierten Einwilligung und der Implementierung von Opt-in-Maßnahmen.[38] Das Protokoll spezifizierte GPC als einen binären Wert, der als Teil eines HTTP-Headers übertragen wird.[39] Die Wiedereinführung von DNT als GPC

33 Vgl. Peter Snyder: *Google's Topics API: Rebranding FLoC Without Addressing Key Privacy Issues*, 26.1.2022, *brave.com/web-standards-at-brave/7-googles-topics-api* (12.12.2022).

34 Vgl. David Eliot, David Murakami Wood: Culling the FLoC: Market Forces, Regulatory Regimes and Google's (Mis)Steps on the Path Away from Targeted Advertising, in: *Information Polity*, Bd. 27, Nr. 2, 2022, 259–274, *doi.org/10.3233/IP-211535*.

35 Vgl. Alex Berke, Dan Calacci: Privacy Limitations Of Interest-Based Advertising On The Web: A Post-Mortem Empirical Analysis Of Google's FLoC, in: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*, 13.10.2022, *doi.org/10.1145/3548606.3560626* (12.12.2022).

36 Vgl. Allison Schiff: Google Delays The End Of Third-Party Cookies (Again), From 2023 To The End Of 2024, in: *Adexchanger.com*, 27.7.2022, *adexchanger.com/privacy/google-delays-the-end-of-third-party-cookies-again-from-2023-to-the-end-of-2024* (26.10.2022).

37 Es sei hier ausdrücklich darauf hingewiesen, dass einer der Autoren auch Autor und Mitwirkender bei ADPC ist.

38 Vgl. Sebastian Zimmeck, Kuba Alicki: Standardizing and Implementing Do Not Sell, in: *WPES '20: Proceedings of the 19th Workshop on Privacy in the Electronic Society*, Virtual Event USA, 2020, 15–20, *doi.org/10.1145/3411497.3420224*.

39 Vgl. *globalprivacycontrol.github.io/gpc-spec* (19.10.2022), wo die technischen Details des Protokolls beschrieben werden.

ist die Folge der Bemühungen von Akademiker*innen, datenschutzfreundlichen Organisationen wie dem EFF sowie einigen großen Medienunternehmen in den Vereinigten Staaten – namentlich der *New York Times* und der *Washington Post*.[40] Während sich die GPC-Spezifikation und der Unterstützer*innenkreis seit der Vorstellung 2020 kaum verändert haben, ist ihre Standardisierung beim W3C zum jetzigen Zeitpunkt nicht absehbar. Zum Zeitpunkt der Erstellung dieses Artikels unterstützten 0,1 Prozent von mehr als 4 Millionen getesteten Websites GPC.[41]

ADPC

Advanced Data Protection Control (ADPC)[42] ist ein vorgeschlagenes Protokoll für die Übermittlung von Einwilligungsanfragen und Datenschutzeinstellungen über den Browser oder das Betriebssystem.[43] Entwickelt wird ADPC in Zusammenarbeit zwischen Forscher*innen und der Verbraucher*innenschutzorganisation noyb.eu, die regelmäßig Unternehmen wegen Verstößen gegen die DSGVO verklagt.

Die ADPC-Spezifikation bezieht sich auf den Rechtsrahmen der DSGVO und die ePrivacy-Richtlinie.[44] Ausgangspunkt der DSGVO ist, dass die Verarbeitung personenbezogener Daten nur dann rechtmäßig ist, wenn sie eine entsprechende Rechtsgrundlage hat; eine Grundlage ist, dass «die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten für einen oder mehrere bestimmte Zwecke eingewilligt hat».[45] Ebenso verlangt die Datenschutzrichtlinie für elektronische Kommunikation die Zustimmung der Nutzer*innen, wenn Daten auf Endeinrichtungen gespeichert oder von Endgeräten abgerufen werden, die über das unbedingt erforderliche Maß hinausgehen.[46] Darüber hinaus haben Nutzer*innen ein Widerspruchsrecht.[47]

Es liegt in der Entscheidung von Nutzer*innen, wie sie die Ausübung ihrer DSGVO-Rechte einem*r Datenverantwortlichen mitteilen – dies kann per E-Mail, durch einen Brief oder eine Schaltfläche auf einer Website erfolgen. Es können aber auch technische Mittel eingesetzt werden:

- Art. 21 Abs. 5 DSGVO sieht ausdrücklich vor, dass «die betroffene Person ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben kann, bei denen technische Spezifikationen verwendet werden».
- In Erwägungsgrund 32 der DSGVO wird auch klargestellt, dass die Einholung und Erteilung einer Einwilligung in verschiedenen Formen erfolgen kann, z. B. durch «das Ankreuzen eines Kästchens beim Besuch einer Website oder die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft», sofern sie Anforderungen wie Information und Eindeutigkeit erfüllt.
- Die vorgeschlagene ePrivacy-Verordnung sieht ebenfalls automatisierte Mittel zur Kommunikation von Präferenzen betroffener Personen vor.[48]

40 Vgl. *globalprivacycontrol.org/orgs#Business* (26.10.2022). Die Website listet die an der Entwicklung und Umsetzung beteiligten Unternehmen.

41 Auf *gpcsup.com* werden tagesaktuelle Zahlen zur Verbreitung von GPC gezeigt.

42 Vgl. Soheil Human: Really Enforceable Solution to Protect End-users Consent & Tracking Decisions (RESPECTeD), in: *Sustainable Computing Reports and Specifications*, Bd. 2022, Nr. 2, 2022, 1–18, *research.wu.ac.at/files/35399528/Soheil_Human_ADPC_Prj4625_RESPECTeD_netidee_call14_Endbericht_Final_Report_Projekte_V06_2.pdf* (31.1.2023).

43 Vgl. Soheil Human: Advanced Data Protection Control (ADPC): An Interdisciplinary Overview, in: *arXiv*, 20.9.2022, *doi.org/10.48550/arXiv.2209.09724* (19.10.2022).

44 Vgl. ebd.

45 Art. 6 Abs. 1a DSGVO: Rechtmäßigkeit der Verarbeitung.

46 Vgl. Art. 5 Abs. 3 DSGVO: Grundsätze für die Verarbeitung personenbezogener Daten.

47 Vgl. Art. 21 Abs. 2 DSGVO: Widerspruchsrecht.

48 Vgl. European Commission: Proposal for the Regulation on Privacy and Electronic Communications (2017/0003 [COD]), 2017, *ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241* (16.12.2022).

Die ADPC-Spezifikation[49] definiert diese automatisierten Mittel, die es Website-Besucher*innen ermöglichen sollen, die Zustimmung für die spezifischen Zwecke zu erteilen oder zu verweigern, bereits erteilte Einwilligungen zu widerrufen sowie der Verarbeitung für Direktmarketingzwecke zu widersprechen. Dies ermöglicht es den Nutzer*innen, Datenschutzentscheidungen einfach über den Webbrowser zu verwalten und anzupassen, wie Anfragen präsentiert und beantwortet werden (z. B. Verwendung einer Browsererweiterung zum Importieren von Listen vertrauenswürdiger Websites). Das Ergebnis könnte vergleichbar sein mit der Art und Weise, wie Websites um Erlaubnis bitten, auf eine Webcam oder ein Mikrofon zuzugreifen: Der Browser verfolgt die Entscheidungen der Nutzer*innen auf Site-by-Site-Basis.

ADPC spezifiziert Attribute für die Einholung, die Erteilung und den Widerruf von Einwilligungen sowie den Widerspruch gegen die Verarbeitung ähnlich wie P3P, aber mit etwas größerer Flexibilität. Technisch erläutert wird im Standard die Verwendung eines Header-basierten Informationsaustauschs in Kombination mit zusätzlichen Informationen – unter Verwendung aktueller Web-Programmierstandards – mit JavaScript und JSON. Im Vergleich zu P3P ist die Spezifikation offener, z. B. in Bezug auf die Definition von Datentypen, die von der Spezifikation ausgenommen sind. Die Entwicklung von ADPC wird größtenteils innerhalb eines akademischen Diskurses vorangetrieben. Als Ziele werden u. a. auch automatische Aushandlungen und eine Anwendbarkeit auf andere Bereiche (wie das Internet der Dinge) gesetzt. ADPC bietet erweiterte und umfangreiche Möglichkeiten für die bidirektionale Kommunikation von Daten, Informationen und Entscheidungen im Zusammenhang mit Einwilligung, kann aber auch zum Senden von binären Attributen wie GPC oder DNT verwendet werden. Darüber hinaus können beide Parteien (d. h. die für die Verarbeitung Verantwortlichen und die betroffenen Personen) die Kommunikation mittels ADPC einleiten. So kann beispielsweise ein*e für die Verarbeitung Verantwortliche*r Datenschutzinformationen und die angeforderten Einwilligungen und Entscheidungen an die betroffene Person übermitteln oder der*die Nutzer*in kann Widersprüche an die datenverarbeitende Stelle senden.

Keines der neueren Protokolle erfährt breite Unterstützung vonseiten der Werbeindustrie. Diese arbeitet eher an der Minimalumsetzung der gesetzlichen Vorgaben. Neben der AdChoices-Website, die nach wie vor zur Verfügung steht, gibt es noch eine neue Website, die im Wesentlichen der AdChoices-Site entspricht, nur andere Farben verwendet und Opt-out-Optionen anbietet, die das CCPA-Opt-out signalisieren sollen.[50]

49 Vgl. *dataprotectioncontrol.org/spec* (26.10.2022), wo Details des Protokolls gezeigt werden.

50 Vgl. *privacyrights.info* (12.12.2022), wo Nutzer*innen ihre Opt-out-Rechte nach CCPA wahrnehmen können.

Die Probleme des Datenschutzes im Internet

Keines der Datenschutzprotokolle, die in diesem Artikel vorgestellt wurden, gilt heute als internetweiter Standard oder hat etwas daran geändert, welche personenbezogenen Daten wie von Internetplattformen verarbeitet werden.

Eine technikzentrierte Analyse würde die Ansätze als ‹gescheitert› betrachten, weil sie weder gültige W3C-Spezifikationen sind noch den Datenschutz für Internetnutzer*innen messbar verbessern. Aber diese Bewertung würde angesichts der Komplexität des Problems zu kurz greifen. Die Entwicklungen der Protokolle erlauben eine Analyse der verschiedenen Akteur*innen und ihrer widersprüchlichen Ziele, die dazu führen, dass Akteur*innen nur in den jeweiligen Modalitäten der Regulierung agieren. Während werbefinanzierte Unternehmen wirksame Datenschutzprotokolle bisher verhindert haben, führt das Scheitern der Selbstregulierung dazu, dass strengere gesetzliche Vorgaben entwickelt werden. Diese brauchen zwar länger bis zur Umsetzung, könnten aber auf lange Sicht eine größere Wirkung haben. Ähnlich wie bei anderen soziotechnischen Systemen ist die Geschichte und die laufende Debatte über Internet-Privacy-Protokolle ein gutes Beispiel für die kontinuierliche Aushandlung zwischen denjenigen, die das Internet betreiben, besitzen und kontrollieren (wollen). Im Folgenden wollen wir eine Reihe von Dichotomien zwischen den bisherigen Protokollen aufzeigen und skizzieren, was wir in Zukunft erwarten können.

Opt-in vs. Opt-out

Obwohl ‹Information› und ‹Einwilligung› sowohl in den USA als auch in der EU zwei zentrale Elemente bei der Regulierung des Datenschutzes sind, gibt es grundlegende Unterschiede bei ihrer Umsetzung. Das EU-Recht sieht Opt-in-Verfahren vor, bei denen personenbezogene Daten nur dann verarbeitet werden, wenn die betroffene Person ausdrücklich und in Kenntnis der Sachlage ihre Einwilligung gegeben hat. Die US-Perspektive, die sich auf die FTC-Leitlinien und Vorschriften wie die des CCPA stützt, tendiert zu Opt-out-Verfahren, bei denen die Nutzer*innen das Recht haben, bestimmten Datenpraktiken zu widersprechen. Opt-in erfordert Protokolle, die eine Reihe notwendiger Informationen und auch Einwilligungen in verschiedenen Abstufungen unterstützen.

Vertrauen vs. Kontrolle

Eine weitere Unterscheidung ist zwischen vertrauensbasierten und kontrollbasierten Ansätzen möglich. Beim vertrauensbasierten Ansatz wird die Verantwortung für das Einhalten des Datenschutzes an diejenigen Unternehmen übergeben, die auch für die Datenverarbeitung verantwortlich sind. Ein Vorteil liegt, wie bei DNT, im vergleichsweise geringen Aufwand des Protokolldesigns. Allerdings ergibt sich ein Interessenkonflikt aufseiten der Unternehmen, die sowohl von den Daten profitieren wollen als auch für die Gestaltung etwa der Einwilligungsdialoge oder die konkrete Umsetzung von Widersprüchen verantwortlich sind. Dies ist umso problematischer, als es keine Mechanismen

gibt, die das Vertrauen zwischen den verschiedenen Parteien stärken könnten, z. B. Transparenzmaßnahmen, durch welche die tatsächlichen Datennutzungspraktiken nachvollziehbar werden.

Bei kontrollbasierten Ansätzen wird versucht, ein Machtgleichgewicht zwischen den Datenverarbeitenden und den Betroffenen herzustellen. Die wichtigste Voraussetzung für eine Verschiebung des Machtgefüges ist die Kommunikation und die Verifikation, d. h. die Möglichkeit, Daten, Verfahren und Benutzer*innenschnittstellen zu kontrollieren und die Einhaltung der angegebenen Datenschutzmaßnahmen zu überprüfen.

Komplex vs. binär

Binäre Protokolle sind einfach zu übernehmen, aber in ihrer Funktionalität und ihren Auswirkungen sehr begrenzt. Aus Sicht von Nutzer*innen scheinen einfache binäre Signale wie DNT oder GPC sinnvoller, allerdings sind sie nicht dazu geeignet, eine informierte Entscheidung zu ermöglichen. Komplexere Protokolle sind schwieriger zu entwickeln, ermöglichen dafür aber auch komplexere Entscheidungen, etwa bestimmte Funktionen von Dritten (wie z. B. eingebettete Videos) zuzulassen, personalisierte Werbung aber zugleich nicht zu erlauben. Während Cookie-Banner die Nutzer*innen von Websites eine Zeit lang vor die Wahl zwischen einer einfachen Zustimmung und einer komplexen Ablehnung durch «erweiterte Einstellungen» stellten, haben Kontrollbehörden diese Praxis mittlerweile für unzulässig erklärt, sodass eine tatsächliche binäre Entscheidung (alles ablehnen oder allem zustimmen) möglich ist, ohne dass komplexere Einstellungen verschwinden müssen.

Global vs. bereichsspezifisch

Ein Grundproblem der informierten Einwilligung ergibt sich aus der gesetzlichen Anforderung, dass sie *spezifisch* sein muss. Das bedeutet, dass jede Website und jeder Dienst in der Lage sein sollte, für den jeweiligen Kontext zu erklären, warum eine Einwilligung erforderlich ist, anstatt globale Optionen wie DNT oder GPC zu verwenden. Bei ADPC etwa kann jede Website eine eigene domänenspezifische Einwilligungsanfrage senden und die betroffenen Personen können selektive Entscheidungen bezüglich der Anfragen treffen. So soll es Nutzer*innen möglich sein, z. B. auf Nachrichtenseiten Werbedienste zu erlauben, die zur Refinanzierung der Seite beitragen, derselben Funktion auf anderen Seiten aber zu widersprechen.

Alternativen zur individuellen Einwilligung

Während die Unterschiede zwischen Opt-in und Opt-out bereits die Frage implizieren, ob eine Einwilligung überhaupt erteilt werden sollte, gibt es

weitere Bedenken gegenüber der Einwilligung zu berücksichtigen. Im EU-Recht werden verschiedene Gründe definiert, nach denen die Verarbeitung personenbezogener Daten möglich ist. Die Einwilligung ist nur eine davon. So dürfen Websites beispielsweise personenbezogene Daten (wie IP-Adressen) verarbeiten, wenn dies aus technischen Gründen erforderlich ist; hierfür ist keine Einwilligung erforderlich. Der Grundsatz der Datenminimierung verlangt, dass bei allen Datenverarbeitungen personenbezogene Daten grundsätzlich nicht oder nur im erforderlichen Umfang verwendet werden. Würden Websites diesen Grundsatz befolgen, wäre in den meisten Fällen keine Einwilligung und damit kein Cookie-Banner notwendig. Nur dort, wo Nutzer*innen Daten eingeben (oder über APIs zur Verfügung stellen), wäre eine ausdrückliche, kontextbezogene Einwilligung erforderlich. Dies ist z. B. der Fall, wenn eine Website den Standort der Nutzer*innen über den Browser abfragt.

Aber auch jenseits der individuellen Datenabfrage muss das Verständnis von Privatheit als etwas, das jede*r Einzelne für einen Moment ‹aufgeben› kann, in Frage gestellt werden.[51] Was immer die Einzelnen an Informationen ‹freigeben›, betrifft auch die Menschen um sie herum. Dies ist leicht nachvollziehbar, z. B. im Zusammenhang mit Bildern, die auf einer Social-Media-Plattform geteilt werden. Es gilt auch für den Bereich der Online-Werbung, in dem Informationen über eine*n Nutzer*in die Privatsphäre anderer beeinflussen. Dies gilt insbesondere für Verfahren wie FLoC. Aber auch wenn beispielsweise zwei Personen dieselbe WLAN-Verbindung und damit dieselbe IP-Adresse nutzen, können sie von den Tracking-Unternehmen als ein Haushalt betrachtet werden, was zur Folge hat, dass ihre Profile wechselweise die für sie geschaltete Werbung beeinflussen.

Einwilligung ist nicht auf Datenschutz beschränkt

Die Einwilligung ist ein grundlegendes Konzept, das derzeit in den meisten Fällen auf einen einzigen Mechanismus reduziert ist, um die Zustimmung zu Datenschutzrichtlinien und Nutzungsbedingungen einzuholen, d. h. zu allen datenschutzrelevanten Praktiken – aber nicht nur zu diesen. Wie in der Literatur erörtert wird, missbrauchen einige Unternehmen die Intersektionalität von Privatheit und Einwilligung in medizinischen Bereichen, um von ihren Nutzer*innen eine Zustimmung unter unlauteren Umständen zu erhalten.[52] Darüber hinaus kann die zunehmende Allgegenwärtigkeit digitaler Tools, die Menschen beeinflussen oder sogar manipulieren (von verschiedenen mobilen Apps über das Internet der Dinge und Augmented Reality bis zu KI-basierten Technologien), die Bedeutung der datenschutzfreien Einwilligung erhöhen. Da es schwierig (oder sogar unmöglich) ist, zwischen (nicht-)datenschutzrechtskonformen Einwilligungen zu unterscheiden, sollten Internet-Privacy-Protokolle explizit in Richtung Datenschutzmanagement entwickelt werden. In

51 Vgl. Beate Rössler: *Der Wert des Privaten*, Frankfurt / M. 2001.

52 Vgl. Soheil Human, Mandan Kazzazi: Contextuality and intersectionality of e-consent: A human-centric reflection on digital consenting in the emerging genetic data markets, in: *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2021, 307–311, doi.org/10.1109/EuroSPW54576.2021.00051; Niklas Kirchner, Soheil Human, Gustaf Neumann: Context-sensitivity of informed consent: The emergence of genetic data markets, in: *Workshop on Engineering Accountable Information Systems*. ECIS, 2019.

Anbetracht dessen scheint ein einzelnes Bit von Opt-out-Attributen nicht ausreichend zu sein, um der umfassenden Komplexität der Einwilligung gerecht zu werden.

Offene Fragen: Durchsetzung und Pluralismus

Es scheint unvermeidlich, dass in den kommenden Jahren mehrere Internet-Privacy-Protokolle nebeneinander existieren. Selbst wenn Regulierungsbehörden spezifischere technische Leitlinien veröffentlichen, wird es wahrscheinlich verschiedene Implementierungen in Browsern oder auf Websites geben. Es ist eine offene Frage, wie die, die Einwilligungen geben und die, die Einwilligungen erbitten, mit unterschiedlichen Protokollen oder sogar widersprüchlichen Signalen umgehen sollten. Hils u. a. haben gezeigt, dass schon jetzt viele Nutzer*innen widersprüchliche Datenschutzpräferenzen senden, wenn sie z. B. einen Browser verwenden, der standardmäßig das DNT/GPC-Signal sendet, die Nutzer*innen aber aus Gewohnheit die Option «Alles akzeptieren» in einem Einwilligungshinweis anklicken.[53]

53 Vgl. Maximilian Hils, Daniel W. Woods, Rainer Böhme: Conflicting Privacy Preference Signals in the Wild, in: *arXiv*, 29.9.2021, doi.org/10.48550/arXiv.2109.14286 (12.12.2022).