Kernkompetenzzentrum
Finanz- & Informationsmanagement

Fraunhofer FIT
Projektgruppe
Wirtschaftsinformatik

Diskussionspapier

Privacy Bots - Digitale Helfer für mehr Transparenz im Internet

von

Niclas Nüske, Christian Olenberger, Daniel Rau, Fabian Schmied

September 2018

erscheint in: Datenschutz und Datensicherheit - DuD

Universität Augsburg, D-86135 Augsburg
Besucher: Universitätsstr. 12, 86159 Augsburg
Telefon: +49 821 598-4801 (Fax: -4899)

Universität Bayreuth, D-95440 Bayreuth
Besucher: Wittelsbacherring 10, 95444 Bayreuth
Telefon: +49 921 55-4710 (Fax: -844710)

www.fim-rc.de

WI-823

Niclas Nüske, Christian Olenberger, Daniel Rau, Fabian Schmied

Privacy Bots

Digitale Helfer für mehr Transparenz im Internet

Seitenlange Datenschutzerklärungen werden im Internet häufig blind akzeptiert. Als digitale Helfer tragen sogenannte Privacy Bots zu einer Stärkung der digitalen Souveränität von Internetnutzern bei, indem sie Datenschutzerklärungen automatisiert auswerten. Dieser Beitrag stellt ein von Nutzern bewertetes Konzept für einen Privacy Bot vor und präsentiert drei Möglichkeiten zur Auswertung von Datenschutzerklärungen.

1 Einleitung

Bestärkt durch zahlreiche Skandale, rückt der Schutz personenbezogener Daten zunehmend in den Fokus der Öffentlichkeit. Für Schlagzeilen sorgte insbesondere der Skandal um Facebook und Cambridge Analytica. Dabei erweckte die Weitergabe personenbezogener Daten von 87 Millionen Facebook-Nutzern vor allem aufgrund der Zusammenarbeit von Cambridge Analytica mit dem Wahlkampfteam des heutigen US-Präsidenten Donald Trump großes Misstrauen. Ein in der Öffentlichkeit weitaus weniger bekannter Datenschutzskandal spielte sich in Österreich ab. Im Jahr 2018 wurde bekannt, dass der Telekommunikationsdienstleister A1 über Jahre hinweg Verbindungs- und Standortdaten von mehreren zehntausend Nutzern unerlaubterweise gespeichert hat[1].

In der Folge legen Kunden heutzutage verstärkt Wert darauf, dass ihre persönlichen Daten hinreichend geschützt sind. Einen gesetzlichen Rahmen hierfür bietet in Deutschland das im Jahr 1990 erstmals in Kraft getretene Bundesdatenschutzgesetz (BDSG). Spätestens seit Mai 2018 müssen sich Unternehmen in den Mitgliedsstaaten der EU zudem an die Richtlinien der europäischen Datenschutz-Grundverordnung (EU-DSGVO) halten.

Im Zuge dieser Entwicklung haben sich seit einiger Zeit auch Unternehmen etabliert, die sich dem Schutz personenbezogener Daten in besonderer Weise verpflichtet fühlen. So verzichtet beispielsweise die Suchmaschine „DuckDuckGo“ im Gegensatz zu anderen Anbietern explizit darauf, personenbezogene Daten der Nutzer zu speichern. Auch etablierte Unternehmen und Konzerne nehmen sich zunehmend der Thematik an. So kündigte der Telekommunikationsdienstleiter „Telefónica“ bereits im Jahr 2016 an, seinen Kunden vollständige Transparenz über die erhobenen personenbezogenen Daten zu bieten[2]. Kunden dürften demnach selbst entscheiden, welche Daten vom Unternehmen genutzt und ggf. an Dritte weitergegeben werden. Stellen Kunden personenbezogene Daten zur Verfügung, sollen sie im Gegenzug attraktive Angebote von Partnerunternehmen erhalten. Die in diesem Zuge gemeinsam mit dem Start-Up people.io entwickelte App „O_2 Get“[3] scheint sich jedoch zum jetzigen Zeitpunkt noch nicht nachhaltig etabliert zu haben und wird von vielen Nutzern kritisch bewertet.

2 Aktuelle Situation

Aufgrund meist sehr langer und kryptischer Datenschutzerklärungen haben Nutzer derzeit häufig keinen ausreichenden Überblick darüber, welche Daten bei der Nutzung eines Internetdienstes erhoben, gespeichert und verarbeitet werden. Da der Aufwand des Lesens und Verstehens einer Datenschutzerklärung meist in keinem vertretbaren Verhältnis zum Nutzen eines Internetdienstes steht, wählen viele Internetnutzer häufig den Weg, die Datenschutzerklärung blind zu akzeptieren. Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) setzt sich daher seit einiger Zeit dafür ein, dass Datenschutzhinweise transparenter dargestellt werden. Unter dem Motto „Datenschutz auf einen Blick“ soll eine nutzerfreundliche, übersichtliche und verständliche Kurzfassung der Datenschutzhinweise idealerweise als sogenannter One-Pager bereitgestellt werden. Allerdings folgen diesem Vorschlag bisher nur wenige Unternehmen. Zusätzlich zeigen erste Studien, dass sich der Kenntnisstand der Internetnutzer durch One-Pager nur geringfügig verbessert[4].

Eine weitere vielversprechende Lösung zur Stärkung der digitalen Souveränität von Internetnutzern und zum Schutz personenbezogener Daten sind sogenannte Privacy Bots. Diese sollen dabei helfen, sich einen schnellen Überblick über die Datenschutzerklärung eines Internetdienstes zu verschaffen. Die Auswertung der Datenschutzerklärungen erfordert demnach nicht einmal mehr das Lesen eines One-Pagers, sondern erfolgt bestenfalls automatisiert und auf Basis individueller Präferenzen der Nutzer. Im Folgenden stellen wir ein Konzept für einen Privacy Bot vor, mit dessen Hilfe es Internetbenutzern ermöglicht werden soll, unterbrechungsfrei im Internet zu surfen und dennoch stets darüber informiert zu sein, wie die besuchten Internetdienste

[1] https://www.heise.de/newsticker/meldung/Datenschutzskandal-bei-Telekom-Austria-3989557.html

[2] https://www.zeit.de/digital/datenschutz/2016-09/mobilfunk-telefonica-bewegungsdaten-kunden-verkaufen-zweiter-versuch

[3] https://blog.telefonica.de/2017/05/kooperation-von-telefonica-next-mit-people-io-app-02-get-ermoeglicht-souveraenen-umgang-mit-eigenen-daten/

[4] https://www.conpolicy.de/data/user_upload/Studien/PolicyPaper_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf

personenbezogene Daten verarbeiten, welche Maßnahmen zum Schutz der Daten getroffen werden und wie diese zu den Präferenzen der Nutzer passen. Hierfür präsentieren wir das Konzept für eine Privacy-Bot-Webseite, die sich gleichzeitig über ein Plug-in direkt in den Browser des Nutzers einbinden lässt, um ihn beim Surfen im Web zu unterstützen.

3 Relevante Dimensionen des Datenschutzes im Internet

Die Grundlage für die Konzeption des Privacy Bots und dessen einfach verständliche Aufbereitung einer Datenschutzerklärung ist eine übersichtliche Unterteilung des Inhalts in bewertbare Kriterien. Bei der Identifikation geeigneter übergeordneter Kategorien stützten wir uns auf den One-Pager[5] des Bundesministeriums der Justiz und für Verbraucherschutz. Dieser soll die förmliche Datenschutzerklärung ergänzen und listet die folgenden vier zentralen Fragestellungen auf: Welche Daten werden gesammelt? Welche Technologien werden verwendet? Wie werden Daten genutzt? Wohin werden die Daten weitergegeben?

Durch eine detaillierte Auswertung beispielhafter Datenschutzerklärungen von fünf Unternehmen identifizierten wir mögliche Ausprägungen, fortan Kriterien genannt, die je einer der vier Kategorien zugeordnet werden können. Die Auswahl der Unternehmen erfolgte mit der Absicht, verschiedene Branchen, Unternehmensgrößen und Innovationsgrade im Hinblick auf Datenschutz abzudecken. Hierfür wurde eine Analyse der Datenschutzerklärungen (beispielsweise von Amazon und der Deutschen Bank) auf Satzebene durchgeführt. In den Datenschutzerklärungen wurden einzelne Kriterien identifiziert und über alle Unternehmen hinweg nach inhaltlicher Ähnlichkeit zu Gruppen zusammengefasst. In Diskussionen des Autorenteams wurden diese Gruppen zu einzelnen, binär zu beantwortenden Fragestellungen verdichtet.

Insgesamt wurden 19 Kriterien identifiziert. Unter die Kategorie „Welche Daten werden gesammelt?“ fallen etwa die Kriterien Benutzereingaben, Standortdaten und Nutzungsdaten. In der Kategorie „Wie werden die Daten genutzt?“ sind beispielsweise die Bereitstellung des Service sowie Werbung als möglicher Zweck vertreten. Bei jedem der 19 Kriterien in den vier übergeordneten Kategorien lässt sich mit einem einfachen „Ja“ oder „Nein“ angeben, wie sich ein Unternehmen datenschutztechnisch positioniert.

4 Mögliche Funktionen und deren Bewertung durch Nutzer

Eine Kernfunktion des Privacy Bots ist die grundsätzlich einmalige, jedoch anpassbare Hinterlegung von individuellen Datenschutzpräferenzen zu den vorgenannten Kriterien. Beispielsweise kann ein Nutzer der Sammlung von Standortdaten zustimmen und gleichzeitig der Nutzung für Werbung widersprechen. Die Zustimmung oder Ablehnung in jeder der 19 Kriterien ergibt in Summe ein Datenschutzprofil des Nutzers, das seine Wünsche zusammenfasst. Jedes der Kriterien kann bei Bedarf durch einfach gehaltene Hilfetexte erklärt werden.

Der Privacy Bot erlaubt dem Internetnutzer das Anlegen mehrerer Datenschutzprofile. Beispielsweise ein relativ sorgloses Datenschutzprofil für Online-Shopping und ein sehr strenges Datenschutzprofil für Online-Banking. Hierdurch trägt der Privacy Bot unterschiedlichen Datenschutzanforderungen Rechnung. Für das Anlegen eines Datenschutzprofils registriert sich der Internutzer einmalig auf der Website des Privacy Bots. Nach Hinterlegung von mindestens einem Datenschutzprofil ermöglicht der Privacy Bot das Prüfen von Internetdiensten im Vergleich zu den hinterlegten Datenschutzpräferenzen.

Der Internetnutzer hat zur Prüfung eines Internetdienstes zwei Möglichkeiten. Entweder trägt er die URL des zu prüfenden Internetdienstes in die *Website des Privacy Bots* ein oder er nutzt das zugehörige *Browser-Plug-in*, das Internetdienste automatisch während des Surfens prüft. Das Konzept der Browser-Plug-ins wird bereits in Form von Werbeanzeigen-Blockern von knapp einem Viertel aller deutschen Internetnutzer erfolgreich verwendet[6]. Prüft der Internetnutzer einen Internetdienst über die Website oder automatisiert im Hintergrund über das Browser-Plug-in, dann prüft der Privacy Bot die Datenschutzerklärung des Internetdienstes und vergleicht diese mit dem vom Internetnutzer hinterlegten Datenschutzprofil. Der Internetnutzer erhält somit auf einen Blick die Antwort auf die Frage, ob der entsprechende Internetdienst entlang des zugehörigen Datenschutzprofils des Internetnutzers handelt. Sofern der Internetdienst in einzelnen Kriterien gegen die Datenschutzpräferenzen des Internetnutzers verstößt, werden die Verstöße in übersichtlicher Form zusammengefasst. Bei Bedarf kann sich der Internetnutzer Details zu den Verstößen ansehen. Für den Internetnutzer entfällt durch den Privacy Bot die aufwändige manuelle Prüfung der Datenschutzerklärungen. Er behält hierdurch seine digitale Souveränität, bzw. gewinnt diese im Vergleich zum gegenwärtig weit verbreiteten „blinden Akzeptieren“ von Datenschutzerklärungen zurück. Er sieht sich durch den Privacy Bot einer erheblich gesteigerten Transparenz hinsichtlich der Erhebung und Nutzung seiner persönlichen Daten gegenüber. Neben der Hinterlegung von Datenschutzpräferenzen und dem Prüfen von Internetdiensten gegen die hinterlegten Datenschutzprofile beinhaltet unser Konzept des Privacy Bots einige weitere Funktionalitäten. So können einmalig geprüfte Internetdienste im Privacy Bot hinterlegt werden. Regelmäßig und automatisch wiederholte Prüfungen der Internetdienste im Hintergrund ermöglichen, den Internetnutzer über konkret geänderte Datenschutzbestimmungen oder besondere Vorkommnisse in Zusammenhang mit dem Datenschutz beim Internetdienst aufmerksam zu machen. Eine spätere Änderung der Datenschutzpräferenzen durch den Internetnutzer würde dann auch eine nachträgliche Überprüfung aller be-

[5] http://www.bmjv.de/DE/Themen/FokusThemen/OnePager/OnePager_node.html

[6] https://de.statista.com/statistik/daten/studie/537062/umfrage/adblocker-rate-in-deutschland/

reits einmal geprüften Internetdienste erlauben. Durch direkte Verlinkung zu den Datenschutzeinstellungen auf Unterseiten eines Internetdienstes wird dem Internetnutzer zudem die Ausübung von Wahlrechten in Zusammenhang mit Datenschutz erleichtert. Der Privacy Bot wird somit zur zentralen Anlaufstelle für Datenschutzeinstellungen eines souveränen Internetnutzers. Einfache und kurze Hilfetexte unterstützen den Internetnutzer ohne ihm den Aufwand von schwer verständlichen, seitenlangen Datenschutzerklärungen aufzubürden – ein ausführliches Nachlesen durch den Internetnutzer ist selbstverständlich weiterhin möglich.

Eine Umfrage unter 78 Internetnutzern und somit auch potenziellen Nutzern des vorgestellten Privacy Bots deutet darauf hin, dass die Funktionalität und tatsächliche Nutzung des Privacy Bots auch von Internetnutzern nachgefragt wird. Den Umfrageteilnehmern wurde ein klickbarer Prototyp des Privacy Bots zur Demonstration zur Verfügung gestellt. Im Anschluss bewerteten die Internetnutzer die Nützlichkeit des Privacy Bots durchschnittlich mit 5,13 (von 7) Punkten. Der vorgestellte Basis-Funktionsumfang des Privacy Bots erreichte eine durchschnittliche Bewertung von 4,79 (von 7) Punkten. Letztlich drückten die Internetnutzer ihre Absicht zur tatsächlichen Nutzung des Privacy Bots mit einer durchschnittlichen Punktezahl von 4,83 (von 7) aus. Die Umfrageergebnisse deuten darauf hin, dass das Konzept des Privacy Bots bereits von einem Großteil der Internetnutzer als Wiederherstellung der digitalen Souveränität im Internet empfunden wird. Der Privacy Bot kann durch seine Funktionalität entscheidend dazu beitragen, das „blinde Akzeptieren“ von Datenschutzerklärung bei Internetdiensten zu verhindern und die Durchsetzung der Wahlrechte in Bezug auf Datenschutz zu stärken.

5 Alternativen zur Auswertung von Datenschutzerklärungen

Für eine breite Anwendbarkeit des Privacy Bots muss jedoch eine große Anzahl an Datenschutzerklärungen möglichst automatisiert auf ihre Konformität mit den Präferenzen des Nutzers hin überprüft werden. Hierfür bieten sich drei Möglichkeiten der Umsetzung besonders an. Datenschutzerklärungen könnten *manuell* durch dedizierte Fachkräfte oder anhand eines Crowd-Ansatzes durch Nutzer des Privacy Bots geprüft werden. Ebenso ist ein automatischer Abgleich der Datenschutzpräferenzen eines Nutzers mit den Angaben eines Internetdienstes und Festlegung von Wahlmöglichkeiten über eine standardisierte *Programm-Schnittstelle* denkbar. Zuletzt ist eine algorithmisch automatisierte Auswertung der Datenschutzerklärungen mit *Text-Mining-Methoden* zu erwähnen. Die drei Alternativen sollen im Folgenden jeweils näher erläutert werden.

5.1 Manuelle Prüfung

Datenschutzerklärungen werden, analog zum Vorgehen der Autoren für diesen Beitrag, manuell von Experten analysiert und für jedes der 19 Kriterien wird das Ergebnis der Konformitätsprüfung festgehalten. Die Präferenzen der Nutzer werden dann mit diesen Auswertungen abgeglichen. Vorteilhaft wäre diese Variante, da durch die manuelle Auswertung durch Experten eine hohe Qualität sichergestellt werden könnte. Als klarer Nachteil der Option schlägt der notwendige Aufwand zu Buche.

Ein crowd-getriebener Ansatz, der die Nutzer des Privacy Bots bei der Auswertung der Datenschutzerklärungen einbindet, könnte eine vielversprechendere Variante der manuellen Prüfung darstellen. Bevor ein Nutzer Zugang zu den Funktionen des Privacy Bots erhält, wird er gebeten, eine bestimmte Datenschutzerklärung oder einen Teil von ihr zu überprüfen. Die Qualität der Auswertungen wird dabei durch eine hinreichend große Zahl von Nutzern und auf Basis der Mehrheitsmeinung sichergestellt. Die manuelle Auswertung im Crowd-Ansatz hat zur Folge, dass die Anzahl der durch den Privacy Bot prüfbaren Webseiten nur nach und nach steigt. Deshalb muss gerade in der Startphase auf eine geeignete Incentivierung geachtet werden.

5.2 Einrichtung einer Schnittstelle

Zwischen dem Privacy Bot und dem genutzten Internetdienst wird eine Schnittstelle geschaffen, die den automatischen Austausch von Informationen über die jeweilige Datenschutzerklärung sowie die automatische Vornahme von Einstellungen entsprechend der Präferenzen des Users erlaubt. Hierfür wird die Liste der in die vier vorgestellten Kategorien gegliederten 19 Kriterien in ein maschinenlesbares Standardformat wie beispielsweise XML oder JSON überführt. Diese wird den Webseitenbetreibern bereitgestellt, die jeweils angeben, ob sie die enthaltenen Kriterien erfüllen oder nicht und ob dem Nutzer ein Wahlrecht eingeräumt wird. Ist ein Punkt optional, so kann er auf Wunsch des Nutzers vom Unternehmen oder dem Betreiber unterlassen werden. Ist er nicht optional, so muss der Nutzer ihn akzeptieren, sofern er den Internetdienst nutzen möchte.

Besucht ein Nutzer nun die Webseite eines Internetdienstes, vergleicht der Privacy Bot die Angaben des Nutzers mit denen des Webseitenbetreibers. Das Ergebnis des Abgleichs wird vom Privacy Bot an den Betreiber zurückgespielt, dessen System anschließend alle optionalen Punkte entsprechend der Vorgaben einstellt. Dem Nutzer wird in seiner Auswertung der Datenschutzpräferenzen somit der optimale erreichbare Stand seines Datenschutzes auf der jeweiligen Webseite dargestellt. Dies ist nur dadurch möglich, dass der Betreiber des Internetdienstes aktiv mit eingebunden ist, sodass auch hier auf eine geeignete Incentivierung geachtet werden muss.

5.3 Textmining

Eine Variante der automatisierten Auswertung ist die Anwendung von Text-Mining-Methoden. Unter Text Mining ist eine Gruppe methodischer Ansätze zu verstehen, die dazu dienen, Texte zu strukturieren, um daraus Informationen zu extrahieren. Die Auswertung der Datenschutzerklärungen mit Text Mining erfolgt in vier Schritten.

Zunächst wird ein Kriterium aus den Datenschutzpräferenzen des Nutzers ausgewählt, zum Beispiel die Sammlung von Standortdaten. Im zweiten Schritt wird die Datenschutzerklärung des Internetdienstes abgerufen und nach relevanten Absätzen durchsucht, die sich auf das ausgewählte Kriterium beziehen. Dies kann entweder mit einer eigenen

Text-Mining-Methode oder durch einen spezialisierten Online-Service passieren. Im dritten Schritt folgt via Text-Mining eine Analyse der identifizierten Textstellen, ob das jeweilige Kriterium erfüllt ist. Hierfür bietet sich die Suche nach Schlüssel-Formulierungen an. Im Falle von Standortdaten könnten solche Formulierungen etwa „verwenden", „verwenden nicht", „Nutzung", „keine Nutzung", „Einsatz", „kein Einsatz", „setzen ein", „setzen nicht ein", „vermeiden", etc. sein. Bei der Verwendung einer statistischen Standard-Methode wie beispielsweise einer Klassifikation, dem Vektorenverfahren oder einer hierarchischen Clusteranalyse ist ein ausreichend großer Trainingsdatensatz zu erstellen, der gängige Formulierungen aus Datenschutzerklärungen und die jeweilige Aussage „positiv/ja/Umsetzung" oder „negativ/nein/keine Umsetzung" enthält. Einmal aus Datenschutzerklärungen abgeleitet, kann der Trainingsdatensatz zur Einschätzung neuer Datenschutzerklärungen weiterverwendet werden. Sobald eine Auswertung der Konformität vorliegt, kann diese Information im letzten Schritt mit den Präferenzen des Nutzers abgeglichen werden.

Dem Vorteil der nach einer ausreichend großen Trainingsphase schnellen und automatisierten Auswertung beliebiger Datenschutzerklärungen stehen beim Text-Mining hohe Implementierungskosten und Anforderungen an das Know-how gegenüber.

6 Monetarisierung im Rahmen eines Geschäftsmodells

Alle drei vorgestellten Verfahren zur Auswertung von Datenschutzerklärungen der Internetdienste sind bereits mit heutigen Methoden umsetzbar und ermöglichen das vorgestellte Privacy-Bot-Konzept von technischer Seite. Jedoch sind alle drei Verfahren mit Aufwand für den Betreiber des Privacy Bots verbunden. Durch die Gestaltung als digitale Plattform stellt der Privacy Bot ein skalierbares Konzept dar. Einmal ausgewertete Datenschutzerklärungen von Internetdiensten stünden allen Nutzern unmittelbar zur Verfügung. Dennoch sind die Implementierung und der Betrieb des Privacy Bots mit finanziellem Aufwand verbunden.

Aufgrund der besonderen Bedeutung für die digitale Souveränität der Internetnutzer, ist für den Privacy Bot ein gemeinnütziges Finanzierungskonzept denkbar, wie es bereits von der Wissensdatenbank Wikipedia erfolgreich umgesetzt wird. Auch eine staatliche Finanzierung zur Sicherung und Durchsetzung der digitalen Souveränität von Internetnutzern ist möglich.

Eine Alternative hierzu ist die Monetarisierung über ein privatwirtschaftliches Geschäftsmodell. Einerseits kann der Privacy Bot ein bestehendes Serviceangebot ergänzen. Zum Beispiel als kostenlose Ergänzung zu den Internetverträgen eines Telekommunikationsanbieters. Andererseits ist der Privacy Bot auch als eigenständiger Service monetarisierbar. Nutzer würden in diesem Fall eine einmalige, regelmäßige oder von der Anzahl der Prüfungen abhängige Gebühr entrichten. Eine Umfrage unter 78 Internetnutzern, denen der Privacy Bot im Detail vorgestellt wurde, ergab erste Anzeichen für eine unterschiedliche Zahlungsbereitschaft. Knapp die Hälfte aller Befragten gab eine grundsätzliche Zahlungsbereitschaft für den Privacy Bot an, wohingegen die andere Hälfte eine kostenfreie Nutzung des digitalen Helfers präferiert.

Vor diesem Hintergrund ist das Angebot des Privacy Bots in einem Freemium-Modell eine mögliche Option. Grundfunktionalitäten wie beispielsweise die manuelle Prüfung von Internetdiensten auf der Website des Privacy Bots würden in einem solchen Freemium-Modell kostenfrei angeboten werden. Der volle Funktionsumfang, beispielsweise die Nutzung des Broswer-Plug-ins zur automatischen Prüfung im Hintergrund oder die Speicherung von geprüften Internetdiensten, wäre in diesem Fall nur gegen Bezahlung nutzbar.

Freemium-Modelle sind bereits erfolgreich von Internetdiensten wie Spotify, OneDrive oder Boxcryptor umgesetzt. Letzterer ermöglicht die vollautomatische Verschlüsselung von Daten in Cloud-Speicherdiensten wie OneDrive, Dropbox oder Google Drive. In der kostenfreien Basisversion sind Grundfunktionalitäten nutzbar; die kostenpflichtige Vollversion enthält den gesamten Funktionsumfang.

Gemeinnütziges Finanzierungskonzept, staatlich finanzierter Service oder privatwirtschaftliches Geschäftsmodell – für unser Konzept des Privacy Bots sind verschiedene Monetarisierungsformen denkbar.

7 Weiterentwicklung zum Datentresor

Das vorausgehend präsentierte Konzept eines Privacy Bots unternimmt bereits einen ersten Schritt zur Stärkung der digitalen Souveränität von Internetnutzern. Sinnvolle Weiterentwicklungen wären die Umsetzung einer Identity-Management-Lösung oder gar eines Datentresors zur individuellen Freigabe von persönlichen Daten.

Sofern der Privacy Bot von einer staatlichen Einrichtung, einer wissenschaftlichen Organisation oder vergleichsweise vertrauenswürdigen Unternehmen wie der Deutschen Telekom oder der Deutschen Post angeboten wird, ist die Umsetzung einer Identity-Management-Lösung eine erste Weiterentwicklung. Zu Beginn verifiziert sich der Internetnutzer einmalig gegenüber des Privacy Bots. Anschließend wäre eine Verifikation des Internetnutzers gegenüber weiteren Internetdiensten ohne erneute Verifikation der Identität denkbar. Traditionelle Verifizierungsverfahren wie PostIdent oder virtuelle Identifikationsverfahren könnten hierdurch womöglich ersetzt werden. Gleichzeitig gehört die Zeitverzögerung bis zur Verifizierung im Internet ab diesem Zeitpunkt dann der Vergangenheit an.

Die Weiterentwicklung zu einem Datentresor wäre eine weitere Alternative zur erheblichen Stärkung der digitalen Souveränität. Der Internetnutzer könnte in diesem Szenario persönliche Daten im Privacy Bot hinterlegen (z.B. Anschrift, Kreditkartendaten, etc.). An zentraler Stelle im Privacy Bot wäre dann die gezielte und individuelle Freigabe von Daten für Internetdienste möglich. Internetdiensten ist der Zugriff auf die Daten nach den Vorgaben des Internetnutzers gestattet, jedoch keine weiterführende Speicherung der Daten. Der Internetnutzer erhält hierdurch nicht nur eine bessere Kontrollmöglichkeit hinsichtlich des Zugriffs auf seine Daten, sondern gewinnt an digitaler Souveränität,

seine Fußabdrücke im Internet nachvollziehbar zu verwalten. Letztlich reduziert die Speicherung persönlicher Daten wie z.B. Kreditkartendaten an einer zentralen Stelle im Privacy Bot das Risiko eines unbefugten Datenzugriffs oder Datenmissbrauchs aufgrund von Entwendung durch Dritte.

Doch auch ohne die genannten Weiterentwicklungen stellt das in diesem Artikel beschriebene Konzept eines Privacy Bots bereits einen wesentlichen Beitrag zur Stärkung der digitalen Souveränität von Internetnutzern dar. Es ist gleichzeitig ein Vorschlag dafür, wie bereits heute verfügbare Technologien zum Schutz persönlicher Daten im Internet eingesetzt werden können.

Autorenbeschreibung

Niclas Nüske, Christian Olenberger, Daniel Rau und Fabian Schmied absolvierten den Elitenetzwerk-Masterstudiengang Finanz- & Informationsmanagement (FIM). Sie promovieren derzeit am Kernkompetenzzentrum Finanz- & Informationsmanagement der Universität Augsburg und der Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT im Bereich Digitalisierung & Datenschutz und wurden 2017 für ihr Privacy-Bot-Konzept durch eine international besetzte, hochrangige Jury von der Deutschen Telekom ausgezeichnet.