H. Langweg, M. Meier, B.C. Witt, D. Reinhardt et al. (Hrsg.): Sicherheit 2018,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2018 13

Anreize und Hemmnisse für die Implementierung von Privacy-Enhancing Technologies im Unternehmenskontext

Eine qualitative Analyse basierend auf Tiefeninterviews mit Privacyexperten

David Harborth[1] Maren Braun[1] Akos Grosz[1] Sebastian Pape[1] Kai Rannenberg[1]

Abstract: Wir untersuchen in diesem Artikel mögliche Anreize für Firmen Privacy-Enhancing Technologies (PETs) zu implementieren, und damit das Privatsphäre- und Datenschutzniveau von Endkonsumenten zu erhöhen. Ein Großteil aktueller Forschung zu Privatsphäre- und Datenschutz (im Weiteren *Privacy*) wird aktuell aus Nutzersicht, und nicht aus der Unternehmensperspektive geführt. Um diese bislang relativ unerforschte Lücke zu füllen, interviewten wir zehn Experten mit einem beruflichen Hintergrund zum Thema Privacy. Die Resultate unserer qualitativen Auswertung zeigen eine komplexe Anreizstruktur für Unternehmen im Umgang mit PETs. Durch das sukzessive Herausarbeiten zahlreicher Interdependenzen der gebildeten Kategorien leiten wir externe sowie unternehmens- und produktspezifische Anreize und Hemmnisse zur Implementierung von PETs in Firmen ab. Die gefundenen Ergebnisse präsentieren wir anschließend in einer Taxonomie. Unsere Ergebnisse haben relevante Implikationen für Organisationen und Gesetzgeber sowie die aktuelle Ausrichtung der Privacyforschung.

Keywords: Qualitative Tiefeninterviews; Qualitative Privacy Forschung; Privacy; Privacy-Enhancing Technologies; Firmenanreize

Also in dem Moment, wo ich sage: "Du hast hier Datenschutz und höhere Anonymität als Premium-Feature", dann hast du automatisch die Frage: „Ja, Standardkunden haben keinen Datenschutz bei euch?"

1 Einleitung

Privatsphäre- und Datenschutz (Privacy) stellen ein Grundrecht in der heutigen digitalisierten Welt dar (siehe dazu auch Datenschutz-Grundverordnung (DSGVO) der Europäischen Union [Re16]). Datenschutzfördernde Technologien (Privacy Enhancing Technologies, PETs), um diese auch umzusetzen gibt es bereits seit einigen Jahrzehnten. Allerdings werden PETs trotz technologischer Ausgereiftheit nur sehr vereinzelt verwendet [Fe01, Te17].
Dabei gibt es prinzipiell drei Akteure, die Anreize für eine entsprechende Verbreitung setzen könnten: Endverbraucher, Anbieter datenschutzbedürftiger Produkte oder Dienste

[1] Goethe University, Chair of Mobile Business & Multilateral Security, Theodor-W.-Adorno Platz 4, 60323 Frankfurt, Germany, david.harborth@m-chair.de

doi:10.18420/sicherheit2018_02

und Regulierer [Hi10, Xu12]. In bisherigen Studien wurde Privacy primär aus Perspektive der Endverbraucher untersucht [SDX11]. Ein Großteil der Endverbraucher räumt dabei anderen Faktoren als der informationellen Selbstbestimmung höhere Priorität ein. Dies zeigt sich beispielsweise an fehlender Zahlungsbereitschaft für Privacy [GA07] und daran, dass Faktoren wie Spaß die Privatsphärebedenken überlagern [DH06]. Rossnagel folgert auf Basis der Diffusionstheorie, dass Nutzer oft die Auswirkungen von PETs nicht erkennen können und deswegen für Anbieter die Vorteile der Einführung von PETs unklar sind [Ro10]. Marktwirtschaftliche Anreize, PETs einzusetzen wurden bisher für Anbieter nur in geringem Umfang untersucht. Rubinstein und der kanadische Datenschutzbeauftragte kommen dabei zum Schluss, dass aufgrund der niedrigen Nachfrage die marktwirtschaftlichen Anreize für Anbieter (oft privatwirtschaftliche Firmen) nicht groß genug sind und der Gesetzgeber Anreize schaffen sollte [Ru11, Te17]. Anreize fehlen möglicherweise auch deswegen, weil viele Geschäftsmodelle die Auswertung persönlicher Daten voraussetzen [Hu14]. Diese Strategie „verlässt“ sich zum Teil darauf, dass Anwender zu träge sind, Opt-out Optionen wahrzunehmen [Te17]. PETs, die Benutzern ein Opt-Out erleichtern würden, stehen dabei dem Geschäftsmodell entgegen.
Zusammengefasst zeigt sich, dass eine Erweiterung der Forschungsperspektive nötig ist. Die eher nutzerzentrierte Forschung muss durch Forschung aus Unternehmenssicht ergänzt werden. Es stellt sich daher die Forschungsfrage, welche Anreize und Hemmnisse Unternehmen dazu bringen bzw. davon abhalten, PETs in ihren Produkten zu etablieren.
Der Rest dieses Beitrags ist wie folgt aufgebaut: Kapitel 2 beschreibt den Forschungsstand und Kapitel 3 die verwendete Methodik. In Kapitel 4 stellen wir eine Taxonomie der Anreize und Hemmnisse für Firmen zur Einführung von PETs vor, die wir in Kapitel 5 diskutieren.

2 Aktueller Forschungsstand

Privacy-Enhancing Technologies stellt einen Sammelbegriff für verschiedene datenschutzfördernde Technologien dar. Borking und Raab definieren PETs als “coherent system of ICT measures that protects privacy [...] by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system” [BR01, S. 1]. Zusätzlich zu den PETs spielen sogenannte Transparency-Enhancing Technologies (TETs) eine wichtige Rolle dafür, dass Bürger bzw. Endverbraucher ihren Privatsphäre- und Datenschutz stärker wahrnehmen. TETs können folgendermaßen definiert werden: “[...] tools which can provide to the individual concerned clear visibility of aspects relevant to these data and the individual’s privacy” [Ha08, S. 205]. Zimmermann [Zi15] gibt einen ausführlichen Überblick am Markt existierender TETs. Die Unterschiede zwischen diesen Technologien sollen in diesem Beitrag nicht näher beschrieben werden, da es weitgehende Überlappungen zwischen ihnen gibt.
Privatsphäre- und Datenschutzthemen werden in bisherigen Studien primär aus Sicht des Individuums untersucht [SDX11]. Für unsere Forschungsfrage sind Studien interessant, die sich mit der Frage beschäftigen, inwieweit Individuen bereit sind, ihr Niveau an Privatsphäre- und Datenschutz zu erhöhen bzw. erhöhen zu lassen. Diese Fragestellung ist deshalb relevant,

da wir argumentieren, dass die Verantwortung für Privatsphäre- und Datenschutz von drei Parteien ausgehen kann, nämlich vom Individuum selbst, von Anbietern datenschutzbedürftiger Produkte oder von Regulierern. Die regulatorische Perspektive klammern wir in diesem Beitrag aus, da wir regulatorische Vorschriften mit möglichen Strafen bei Verstößen nicht als durch den Markt gegebenen Anreiz betrachten.
Forschung zu Privacy auf individueller Ebene hat gezeigt, dass Menschen angeben, sich um ihre Privatsphäre im Internet zu sorgen. Jedoch handeln sie dann entgegen ihrer vorherigen Aussagen und veröffentlichen beispielsweise zahlreiche persönliche Informationen in sozialen Netzwerken. Aktuelle Forschung erklärt dieses Verhalten einerseits mit einer Art kognitiver Dissonanz, die beim Thema Privacy hervortritt (vgl. Privacy Paradox [NHH07, SGB01]). Dieser Erklärung entgegenstehend sehen zahlreiche andere Forscher einen bewussten Trade-Off im Sinne eines Austausches eines speziellen Nutzens (kostenfreie Dienstleistung, Anerkennung, etc.) gegen Daten, auf den Nutzer sich einlassen (vgl. Privacy Calculus [DH06, DT15, DM16]). Weitere Forschung zeigt, dass Individuen neben dieser Divergenz von geäußerter Einstellung und beobachtbarer Handlung nur wenig Kosten (zeitlich und monetär) für ihre Privatsphäre tragen möchten [GA07].
Insbesondere der letzte Punkt wirft die Frage auf, inwieweit es unter diesen Voraussetzungen möglich ist, PETs profitabel am Markt zu etablieren. Daher ist es relevant, die Unternehmensperspektive auf Anreize für Unternehmen zu beleuchten. Die bisherige Forschung in diesem Gebiet ist nicht so reif wie im Gebiet der Forschung zu Privacy und Individuen [SDX11]. Einige der Artikel beschäftigen sich mit den Konsequenzen von Privatsphäre- und Datenschutzverletzungen in Firmen [AFT06] und wie Firmen mit diesen Verletzungen umgehen können [CKJ16]. Relativ viele Beiträge untersuchen, inwieweit Privacy ein kompetitiver Vorteil ist und sich in Geschäftsmodelle integrieren lässt [Ho14, CMHD15, Li11].

3 Methodik

In diesem Kapitel besprechen wir die verwendete qualitative Forschungsmethodik. Wir folgen diesem explorativen Ansatz, da bisherige Forschung unsere Forschungsfrage unzureichend adressiert hat. Im ersten Schritt haben wir einen semi-strukturierten Leitfadenfragebogen entworfen. Basierend auf dem semi-strukturierten Fragebogen werden die Teilnehmer durch das Interview geführt. Semi-strukturiert bedeutet in diesem Zusammenhang, dass das Interview maßgeblich durch die Interaktion und die Antworten des Befragten beeinflusst wird. Der Fragebogen hält nur besonders relevante Fragen fest, die auf jeden Fall angesprochen werden wollen. Dies hat den Vorteil, möglichst tiefe Einblicke und ausführliche Antworten vom Teilnehmer erhalten zu können. Der Fragebogen kann in drei inhaltliche Oberthemen aufgeteilt werden. Zuerst werden allgemeine Fragen zur Person und zum Unternehmen gestellt. Darauf folgen Fragen zu Privacy und PETs. Der zweite Teil deckt technische Fragen zum Status Quo und zu eventuellen zukünftigen Entwicklungen ab. Der dritte Teil behandelt ökonomische und gesellschaftliche Fragestellungen.
Für die Beantwortung unserer Forschungsfrage haben wir Experten und Professionals befragt, die mit Privacy-Enhancing Technologies (PETs) in ihren Unternehmen zu tun haben,

oder bei deren Produkten oder Dienstleistungen Privacy eine besondere Rolle spielt. Die Experten stammen von Firmen, die direkt PETs anbieten, oder in denen Privacy eine wichtige Rolle im Nutzenversprechen spielt. Als Beispiele hierfür sind der Telekommunikationssektor, Paymentprovider oder eCommerce Solutions Provider zu nennen. Wir haben zehn Interviews geführt und analysiert, wobei die Dauer zwischen 44 Minuten und 180 Minuten variiert. Die demografischen Informationen finden sich in Tabelle 2.
Die Interviews wurden alle aufgezeichnet und anschließend Wort für Wort transkribiert. Die Transkriptionen wurden daraufhin mit dem sog. offenen Kodieren und selektiven Kodieren analysiert [GS67, Ch14, St13]. Das offene Kodieren ist der erste Schritt der Datenauswertung und orientiert sich nah an den Daten (den Transkripten). Im nächsten Schritt werden Kodes zusammengefasst und abstrahiert (selektives Kodieren). Diese Schritte werden für jedes Interview einzeln durchgeführt und anschließend zwischen den Interviews. Diese sogenannte komparative Methode [GS67, Ch14, St13] ist ein elementarer Bestandteil der qualitativen Forschungsmethodik. Durch ständiges Vergleichen zwischen den Interviews, leiten wir abstrakte Kategorien aus den Daten ab, die ein vielfältiges Bild der Anreize und Hemmnisse liefert. Diese Kodierungsschritte wurden von zwei Autoren durchgeführt, um eventuelle Diskrepanzen in der Analyse der Daten festzustellen und zu lösen.

4 Resultate

Wir stellen in diesem Abschnitt das Kategoriensystem vor, welches elementar wichtig für eine logische und aufeinander aufbauende Strukturierung der Ergebnisse ist. Unsere übergeordnete Zielsetzung lag bei diesem Prozess darin, die Unternehmensperspektive in Bezug auf PETs nachzuvollziehen und zu verstehen. Da die Interviewteilnehmer sehr vielschichtige, sowohl vergleichbare und aufeinander aufbauende, als auch gegensätzliche, Stellungen bezogen, leitete sich hieraus eine argumentative Gliederung der relevanten Themenkomplexe ab. Diverse Querbezüge und Wechselwirkungen markieren damit ein interdependentes Gefüge, in welchem Unternehmen Anreize und Hemmnisse für die Implementierung von PETs betrachten. Ein Interviewteilnehmer fasst diese komplexen unternehmenszentrierten Abwägungsentscheidungen im Rahmen des Einsatzes von Privacy-Enhancing Technologies in den folgenden Worten zusammen: "*Ja, es [meint: PETs] soll funktionieren. Ja, und die, die es betreiben, sollen davon leben können. Ja, das soll so sein, aber es soll so sein, dass eben die Kontrolle, Transparenz und Nutzbarkeit breit akzeptierbar ist*" (D).

4.1 Technische Optimierung

Der Großteil der Interviewpartner gab an, dass PETs dienlich sind, um allgemein Unternehmensprozesse auf technischer und organisatorischer Ebene zu optimieren, "*dass man eben vor allem einen technologischen Vorsprung hat*" (B). Die spezifische Modellierung und Funktionalität der Technologie fördert dabei, dass Abläufe im Unternehmen unterstützt, vereinfacht und auch bedarfsgerecht angepasst werden können, was einen technologischen Ansatz zur Realisierung von Privacy-Maßnahmen im Unternehmen darstellt.

Tab. 1: Taxonomie

1. Technische Optimierung	1. Integration in den Geschäftsprozess	
	2. Datenmanagement und -vermeidung	
2. Geschäftsmodell	1. Weiterentwicklung Services	1. Kundenanforderung
		2. Vereinfachung / Convenience
		3. Awareness / Visualisierung
	2. Erweiterung Kundenkreis	1. Kerngruppe mit Privacybedürfnis
		2. Massenmarkt und Segmentierung
	3. Entwicklung neuer Geschäftsmodelle	1. Premiumservice
		2. Wirtschaftlichkeitsabwägung
	4. Positionierung für die Zukunft	
3. Unternehmens-wahrnehmung	1. (Technische) Sicherheit	
	2. Profilierung durch PETs	
	3. Geschäftsethik	

Integration in den Geschäftsprozess. Notwendige Bedingung für die Erwägung einer PET-Implementierung in den Geschäftsprozess ist, inwiefern Tools auf technischer Ebene auf relevante Prozesse abbildbar sind bzw. ob der Kostenaufwand in einem für angemessen erachteten Rahmen liegt: "*Gibt es so etwas? Wieso brauche ich so etwas? Wie kriege ich so etwas? Wie installiere ich so etwas? Und dann, wie setze ich es richtig für meinen Gebrauch ein?*" (H). Das Fehlen einer gesicherten Informationsgrundlage diesbezüglich wurde allerdings bemängelt: "*Man kann sich Vieles vorstellen, ob es dann in der Realität umsetzbar ist, ist dann die Frage*" (A).

Datenmanagement und -vermeidung. PETs können ein vereinfachtes und adäquates Datenmanagement gewährleisten, um darüber hinaus auch für den Geschäftsprozess nicht notwendige Daten vermeiden zu können. Dies kann letztlich auch mit dem gänzlichen Verzicht personenbezogener Daten einhergehen. Ein zentraler Anreiz für die Implementierung von PETs ist daher, dass Unternehmen die unmittelbare Entscheidungshoheit über Erhebung und Aggregation von Daten erlangen. Ein Interviewpartner erörtert, dass "*man immer von irgendwelchen Daten irgendwelche Rückschlüsse ziehen kann*" (A), weshalb Daten außerhalb ihrer jeweiligen Nutzung und Notwendigkeit als ein zusätzliches Geschäftsrisiko bewertbar sind. Ein weiterer Interviewpartner leitet aus der Vermeidung von Daten einen positiven Nutzen für Unternehmen ab: "*Wenn die Daten zum Beispiel nur dort sind, wo sie überhaupt gebraucht werden, dann brauche ich da nicht irgendwie auf den anderen Systemen, wo sie nicht gebraucht werden, erstmal Verschlüsselungen und Maßnahmen [mit]ergreifen*" (F). Die Möglichkeit auf schlankere und einfachere Unternehmensabläufe wurde ferner ebenfalls herausgearbeitet. Andererseits bieten unverschlüsselte personenbezogene Daten den Vorteil, eindeutig einem angelegten Profil und jeweiligen geschäftlichen Aktivitäten zugeordnet werden zu können: "*[Ein Klarname] ist natürlich einfacher, um Transaktionen zuzuordnen, um Versand beispielsweise einem gewissen Kunden zuzuordnen. Aber grundsätzlich wäre das auch über ein Pseudonym schon machbar*" (B).

4.2 Geschäftsmodell

Die Kategorie Geschäftsmodelle stellte sich im Rahmen unserer Auswertung als umfangreichste Kategorie dar (Schlüsselkategorie). Auf dieser Ebene wurden sowohl die stärksten Anreize als auch Hindernisse an die Forschenden herangetragen. Die zahlreichen Freiheitsgrade und Gestaltungsoptionen in Zusammenhang mit PETs wurden als primär ausschlaggebend für die hohe Schwingungsbreite des erwarteten Geschäftserfolgs bewertet. Der vorliegende Status quo wurde von einem Interviewpartner durchaus auch optimistisch aufgefasst: "*Wir können mit [PETs] glaube ich völlig neue Geschäftsmodelle aufbauen, die der Markt bisher überhaupt noch nicht kennt. [...] Wir wollen tatsächlich ein paar Schuhe von A nach B bringen anonym. Das kann aber auch was völlig anderes sein*" (E).

Weiterentwicklung Services. Unsere Ergebnisse zeigen, dass die Implementierung von PETs auch dazu beitragen kann, dass Unternehmen bestehende Services weiter in Richtung Datenschutz entwickeln können und damit in spezifischen Marktstrukturen einen Wettbewerbsvorteil generieren können.

KUNDENANFORDERUNG. Wie stark Kundenanforderungen hinsichtlich des Privatsphäre- und Datenschutzniveaus ausgeprägt sind, steht in Verbindung damit, welche Kundenstruktur gegeben ist und auf welche Segmente künftig spekuliert wird. Aus den Interviews ging sowohl hervor, dass es Kunden gibt, die ein großes Interesse hegen, sich zu schützen und sich diesbezüglich mit Nachfragen wie Ansprachen an Unternehmen wenden, als auch die Auffassung der Interviewpartner, dass Privacy keine bzw. eine eher untergeordnete Rolle beim Gros der (potenziellen) Kunden spielt. Eine etwas andere Konnotation sehen wir indes darin, dass Kunden einen ausreichenden Privatsphäre- und Datenschutz selbstredend erwarten, dies allerdings nicht zwingend explizit an Unternehmen herangetragen: "*Da erwartet der Kunde auch, dass da gewisse Schutzmechanismen passieren. [...] Und das passiert auch. Und das bezahlen sie auch implizit*" (D).

VEREINFACHUNG UND CONVENIENCE. "*Jetzt speziell auf das Internet gesehen, [. . .] jeder gibt irgendwie Daten dort preis. [...] Ist halt oft schwer, nur das preiszugeben, was man möchte, weil man eben doch oft Dinge preisgibt, von denen man nicht weiß oder in dem Moment, wo man sie preisgibt, eben nicht weiß, was damit geschieht letztendlich*" (B). Im Anschluss an diesen Problemaufriss fassen wir unter dieser Kategorie, dass (mögliche) Kunden unbefangen eine Geschäftsbeziehung mit einem Anbieter eingehen und aufrechterhalten können, da entsprechende Services hinsichtlich ihrer Privacy-Einstellungen verbessert wurden. Den Konsumenten wird dadurch kommuniziert, dass sensible Daten nicht erhoben bzw. diese ausreichend durch jeweilige Mechanismen geschützt werden: "*[Die Kundenansprache] könnte man jetzt so machen: '[...] Wir haben jetzt eine neue Technologie [...] installiert [...] und die Möglichkeit schützt deine privaten Daten. Sonst bleibt für dich alles gleich.' [...] Es ist leicht verständlich. Er muss die Technologie auch nicht verstehen*" (A). Andererseits betrachtete ein Teil der Interviewpartner Einfachheit und Bequemlichkeit unter dem Gesichtspunkt, dass datenschutzfördernde Tools aus ihrer Sicht eher einen Mehraufwand für Kunden darstellen: "*Letztendlich, warum wir die Daten speichern möchten oder teilweise speichern wollen, ist eben, um dem Kunden zu vereinfachen, dass er beim nächsten Mal zum Beispiel dann nichts mehr eingeben muss. [...] Also letztendlich ist*

das immer so eine Abwägung zwischen Privatsphäre und zu viele Daten sammeln oder Einfachheit, also im Grunde eben ein möglichst einfaches Interface zu bieten" (B).

AWARENESS UND VISUALISIERUNG. Unternehmen wurde eine wichtige Rolle dabei zugesprochen, auf die Privacy-Thematik aufmerksam zu machen und (potenzielle) Kunden hierfür zu sensibilisieren. Die Interviewteilnehmer erachteten dies als angemessene Maßnahme, um Nachfrage auf diesem Gebiet zu generieren. Gleichzeitig sah ein Befragter Firmen in dieser Hinsicht nicht in der Verantwortung: "*Wir brauchen Awareness von den verschiedenen Segmenten, die es brauchen*" (H). Weiterhin wurde eine geeignete Form der Visualisierung als substanziell eingestuft, um Nutzern die Vorteilhaftigkeit von PETs vor Augen zu führen: "*Irgendwo hätte ich schon gerne als Endteilnehmer, wenn ich schon bezahle, ja, warum bezahle ich eigentlich? Also da muss irgendwie so eine Beweisnotwendigkeit sein*" (D). Inwiefern ein Premium- oder Upselling-Preismodell als sinnvoll zu erachten ist und ob ein Zusatznutzen wie die genannte Visualisierung einen attraktiven Trade-off für Kunden darstellt, werden wir im Abschnitt "Premiumservice" näher diskutieren.

Erweiterung Kundenkreis. Eine Privacy-freundliche Ausrichtung von Unternehmen kann neue Kundenmärkte öffnen und ein Alleinstellungsmerkmal darstellen.

KERNGRUPPE MIT PRIVACY-BEDÜRFNIS. Die Erweiterung des Kundenkreises ist ein häufig von den Befragten formulierter Anreiz für Unternehmen, PETs zu implementieren. Im Kern fielen darunter Personen, bei denen ein Privacy-Bedürfnis bereits überdurchschnittlich stark ausgeprägt ist: "*Ich adressiere genau diese Lücke. Ich adressiere die Freaks, ich adressiere die Nerds, ich adressiere diejenigen, die mehr Privacy Awareness haben, als die anderen*" (G). Nicht nur technikaffine und -interessierte Privatpersonen sind für die Befragten Teil dieser Kategorie, sondern auch Forschungs- und Entwicklungszentren sowie bestimmte Unternehmen. Neben intrinsischen Motiven PETs nachzufragen, spielen für Geschäftskunden häufig auch rechtliche Vorgaben zum Datenschutz eine zentrale Rolle.

MASSENMARKT UND SEGMENTIERUNG. Interviewteilnehmer lieferten sehr nuancierte Aussagen, bezüglich der möglichen Eignung von PETs im Massenmarkt (Primär- und Sekundärnutzen betrachtend). Wir haben diese vielfältigen Blickwinkel aufgegriffen, da sie im Rahmen ihrer jeweiligen Logik nicht zwingend als Widerspruch zu betrachten sind. Ein Potenzial zum Massenmarkt wurde unter anderem beschrieben, um ein besonders hohes Privatsphäre- und Datenschutzniveau als wünschenswerten Idealzustand in den Vordergrund zu stellen. Ein Befragter gab in diesem Zusammenhang an, dass "*jeder, der eine Kundenbeziehung hat*" (D), PETs im Sinne seiner Kunden implementieren sollte. Es ließ sich zudem der Konsens herauslesen, dass dies vom Großteil der Nutzer nicht explizit gefordert und nachgefragt wird, sondern eher akzeptiert, dann aber auch als positiver Nutzen empfunden wird: "'*Kann ich da Datenschutz einschalten? Ja oder nein?' Und dann glaube ich schon, dass viele Leute sagen: 'Joa, einschalten. Datenschutz ist immer gut*'" (G). Des Weiteren wurde Massentauglichkeit darin gesehen, dass PETs in bereits bestehende Produkte als Sekundärnutzen implementiert werden: "*Welche PETs setzen sich bisher im Massenmarkt durch? Nur eigentlich in Begleitung mit anderen Services eben*" (C). Als integraler Baustein etablierter Leistungen können PETs dadurch gar ohne aktives Nutzereinverständnis und ohne konkrete Nachfrage auf dem Massenmarkt etabliert werden. Gleichzeitig wurde die Notwendigkeit angeführt, in Marktsegmente zu unterscheiden: "*Seit Jahren habe ich*

gesagt, argumentiert, dass Mass Marketing ein Fehler ist. [...] Die Unterschiede zwischen den Anforderungen von den verschiedenen Segmenten [...] sind so groß. Verschiedene Leute brauchen unterschiedliche Unterstützung" (H). Diese Aussage steht in Verbindung damit, dass im Rahmen der geführten Interviews zahlreiche potenzielle Nutzergruppen genannt wurden: Unternehmen verschiedener Größe, Forschungsinstitutionen, öffentliche Einrichtungen, Privatpersonen, für die der Schutz der Privats- und Intimsphäre von hoher Bedeutung ist, beispielsweise, wenn sie "*in einem speziellen Segment sensible Produkte*" (A) erwerben möchten. Eine dritte Gruppe von Befragten bewertete einen größeren Kundenkreis hingegen als unrealistisch: "*Ich denke, dass es [meint: PETs] in gewisser Weise schon auch ein Nischenmarkt ist, also dass es nicht unbedingt massenmarkttauglich ist, weil einfach zu vielen Menschen die Privatsphäre da zu unwichtig ist [. . .] beziehungsweise unwichtig genug, um keine extra Mühen auf sich zu nehmen*" (B).

Entwicklung neuer Geschäftsmodelle. Neben der Erschließung neuer Kundenmärkte, kann eine datenschutzfreundlichere Ausrichtung neue Geschäftsmodelle ermöglichen.

PREMIUMSERVICE. Die Interviewten hatten keine eindeutige Meinung, inwiefern sich durch die Implementierung einer PET ein Premium- oder Upselling-Service geschäftlich sinnvoll ist. Ein Befürworter dieses Preismodells erklärte: "*Ja, es [meint: PETs] kostet was. Das ist wieder der berühmte Punkt: Es gibt etwas kostenlos, dann ist es aber eine mildtätige Spende, wo jemand sagt: 'Jawohl, ich spende das dafür, dass es auch wirklich kostenlos ist, so.' Alle anderen Sachen haben irgendwo ihren Trade-off. [. . .] Wir können genau sagen: 'Das kostet es, das bringen wir. Macht mit oder lasst es bleiben'*" (D). Allerdings können bestehende Leistungen des Unternehmens, die eventuell um keine datenschutzfördernde Technologie erweitert wurden, degradiert werden: "*Du versuchst ein Premium-Feature zu positionieren, aber gleichzeitig qualifizierst du alle anderen [angebotenen Services] ab und bringst die in eine Situation, dass du dich für die dann rechtfertigen musst: 'Warum kriegen das nicht alle?' Und die zweite Frage ist: Wer ist bereit für ein solches Premium-Feature zu bezahlen? Es ist dann irgendwas Exklusives*" (G). Daran anknüpfend bezieht ein Interviewteilnehmer folgende Position: "*Die monetären Kosten muss [das Unternehmen] kalkulieren*" (F).

WIRTSCHAFTLICHKEITSABWÄGUNG. Ohne Premium-Services müssen Unternehmen die Kostendeckung einer PET-Implementierung anderweitig garantieren, zum Beispiel durch Absatzsteigerung: "*Wir würden nur über Mengensteigerungen verdienen, weil wir dieses System anbieten*" (A). Alternativ ist es auch möglich, die Konversionsrate durch PETs zu steigern: "*Dem Hersteller nutzt es dann, wenn die Kunden einen Nutzen dahinter sehen und wenn es vielleicht dieser winzige Ausschlag ist, der eine Kaufentscheidung beeinflusst*" (G). Neben diesen quantifizierbaren Aspekten spielen weitere Faktoren, z.B. eine heuristisch orientierte Kosten-Nutzen-Analyse, eine zentrale Rolle in den jeweiligen Abwägungsentscheidungen. Diese gehen mit einer negativen Konnotation von Datenerhebungsvermeidung einher, bspw. durch Betrugsfälle: "*Ich denke [Unternehmen] werden auf jeden Fall erstmal Vorbehalte gegen so etwas [meint: PETs] haben, eben dadurch, dass sie befürchten, für irgendwelche Betrugsfälle oder so keinen greifbaren Kontakt irgendwie zu haben*" (B). Zum anderen wurde mehrfach folgende Befürchtung akzentuiert: "*Die [Unternehmen] haben natürlich kein Interesse an einem Pseudonym, denn die wollen ja Daten, Profile, Bewegungsprofile erstellen, weil das bares Geld ist*" (I).

Positionierung für die Zukunft. Zum einen betonten Befragte die Möglichkeit des Alleinstellungsmerkmales von PETs: "*Das wäre das Alleinstellungsmerkmal irgendwie für uns auch, [ein Produkt] eben anzubieten, [das] die Identität des Kunden schützt, was es eben zurzeit noch nicht so gibt, ja, also vor allem eben auch irgendwie dadurch einen Wettbewerbsvorteil zu gewinnen*" (B). Allerdings schwindet dieser Vorteil eventuell, wenn eine kritische Masse an Wettbewerbern ebenfalls vermehrt PETs implementieren oder Wettbewerber mit bedeutenderer Marktmacht bestimmte Schutztechnologien als neuen „Standard" etablieren: "*Die [meint: https-Verschlüsselung] setzt sich durch, langsam, weil tatsächlich große Konzerne auch dahinter stehen und das jetzt auch forcieren*" (C). Zum anderen wurde PETs eine präventive Wirkung beigemessen, um „Datenschutzskandale" zu vermeiden: "*Man [hat] das schon noch natürlich immer im Hinterkopf, weil man irgendwie auch ganz sicher nicht das Unternehmen sein möchte, was irgendwie in den Schlagzeilen ist, jetzt irgendwie auffällt dadurch, das die Privatsphäre nicht schützt.*" (B).

4.3 Unternehmenswahrnehmung

Privatsphäre- und Datenschutztechnologien verfügen über das Potenzial, sowohl die externe als auch die interne Wahrnehmung des Unternehmens zu beeinflussen.

(Technische) Sicherheit, Vertrauen und Qualität. Für das Vertrauensverhältnis zwischen Geschäftspartnern spielt das Verständnis der jeweiligen Technologie nur eine sekundäre Rolle. Die positive Wahrnehmung entstammt vorranging der impliziten Gefühlsebene: "*Heute verkaufen sich Sachen gut [...] indem gesagt wird: 'Wir machen das nach deutschen Datenschutzrechten [...].' Das verstehen die Leute. Die kennen überhaupt null Details dazu, aber die sagen sich: 'Okay. Wenn das nach deutschem Datenschutzding ist, dann passt das'*" (E). Die durch PETs gewährleistete Vertrauensfestigung kann sich dabei positiv auf den Ruf des Unternehmens niederschlagen: "*Ich sehe es als Qualitätsmerkmal*" (E).

Profilierung durch PETs. Die Kopplung von PETs an das bekannte Dienstangebot des Unternehmens stellt zudem ein kommunizierbares Alleinstellungsmerkmal dar, wie einer der Befragten erläuterte: "*Man kann es als Werbezweck verwenden. [...] Ich unterscheide mich damit von anderen. Das muss jetzt nicht sein, dass das so einen wahnsinnigen Zusatznutzen hat, es ist einfach ein Marketing-Effekt, den ich damit verbinden kann*" (C). Dieser allgemeine Werbeeffekt fördert dann nicht nur das reguläre Angebot, sondern auch die Reputation des Unternehmens: "*Ich glaube du kannst es [meint: mit PET-Implementierung auch Profitabilität sichern] nur machen, wenn du das als Add-on zu deinem Produkt [anbietest]. [...] Dann sagst du: 'Okay, ich investiere jetzt halt mal, weil das bringt mir vielleicht etwas in meinem Ansehen, in meinem Ruf, in meiner Zahl der [Kunden]'*" (I).

Geschäftsethik. Drei ethische Momente des unternehmerischen Handelns heben sich im Hinblick auf Privatsphäre- und Datenschutztechnologien aus den Interviews hervor. Erstens wird die These angeführt, dass Technologien und ihre Nutzung unabhängig von moralischen Wertepositionen gegeben sind: "*Es existiert, es ist keine Frage, keine moralische Frage. Es gibt Anonymität, das ist ein Konzept und es kann für verschiedene Zwecke benutzt werden*" (H). Diese an sich neutrale Auffassung von PETs kann polarisierenden Darstellungen gegenübergestellt werden. So können sich daraus moralisch vertretbare

Schritte zur informativen Sensibilisierung ergeben, jedoch auch verwerfliche, wie zum Beispiel eine einseitige, überspitzte Beängstigungskampagne. Diese können sich gar als geschäftsschädlich herausstellen: "*Natürlich, ich nutze es, ich habe Angst, aber ich weiß auch, dass ich das Produkt nur nutze, weil ich Angst habe. Es macht es jetzt auch nicht unbedingt so wahnsinnig sympathisch*" (C). Letztlich stehen moralische Aspekte der ökonomischen "Rationalität" von Firmen entgegen: "*Ich investiere jetzt in etwas und [...] ich mache das erst einmal, weil ich der Meinung bin: 'Das ist richtig und es hilft und es ist das Richtige zu tun und langfristig profitiere ich vielleicht auch davon, vielleicht nicht finanziell.' Das macht kein Unternehmen*" (I).

5 Diskussion und Schluss

Basierend auf der qualitativen Auswertung von zehn Tiefeninterviews mit Privacyexperten haben wir eine Taxonomie der Anreize und Hemmnisse für die Implementierung von PETs im Unternehmenskontext entwickelt.
Gemäß der Taxonomie spielen die mit Geschäftsmodellen verbundenen Anreize eine wichtige Rolle. Wie bestehende Literatur kommen wir allerdings zum Schluss, dass es Bedarf für weitere Forschung in dem Bereich zu Privatsphäre- und Datenschutz speziell im Unternehmenskontext gibt. Beispielsweise argumentiert Rubinstein [Ru11], dass die marktwirtschaftlichen Anreize für Firmen nicht gross genug sind und eine flächendeckende Verbreitung von PETs nur aufgrund von Initiativen des Gesetzgebers stattfinden wird. Ein weiteres vielversprechendes Thema für zukünftige Forschung besteht in dem Vergleich von Evaluierungen und Meinungen verschiedener Privacyexperten. Unsere Ergebnisse zeigen in einigen Bereichen kein klares Bild, da die Aussagen teilweise weit auseinander gehen. Befragte haben einerseits sehr unterschiedliche berufliche (Unterschiede in Firmen bezüglich Marktumfeld und Marktgröße) und private Hintergründe und andererseits sind ihre Positionen entweder ethisch oder praxisorientiert.
Wir tragen zur aktuellen Privacyforschung auf drei Wegen bei. Erstens haben wir Privacy im Unternehmenskontext, und nicht auf individueller Ebene, untersucht [SDX11]. Zweitens haben wir eine empirische, nicht normative, Studie durchgeführt, die auf einem Sample mit deutschen Interviewteilnehmern basiert. Zum Großteil ist Privacyforschung normativ und basiert auf Stichproben mit US-amerikanischen Teilnehmern [BC11]. Drittens haben wir mit einer qualitativen Methodik ein unterrepräsentiertes Thema explorativ von verschiedenen Dimensionen erforscht. Zusammenfassend zeigen unsere Ergebnisse, dass es durchaus Anreize für Unternehmen (abgesehen von Regulierung) geben kann, datenschützfördernde Technologien und Strukturen in ihren Geschäftspraktiken zu implementieren und damit dem Datenschutz zukünftig mehr Relevanz zu geben.

6 Acknowledgments

Diese Forschung wurde vom Bundesministerium für Bildung und Forschung (BMBF) unterstützt (Zuwendungsnummern 16KIS0371 and 16KIS0515).

Literaturverzeichnis

[AFT06] Acquisti, Alessandro; Friedman, Allan; Telang, Rahul: Is There a Cost to Privacy Breaches? An Event Study. In: International Conference on Information Systems (ICIS). 2006.

[BC11] Bélanger, France; Crossler, Robert E.: Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly, 35(4):1017–1041, 2011.

[BR01] Borking, John J.; Raab, Charles: Laws, PETs and Other Technologies for Privacy Protection. Journal of Information, Law and Technology, 1:1–14, 2001.

[Ch14] Charmaz, Kathy: Constructing Grounded Theory. Sage Publications, London, 2nd editio. Auflage, 2014.

[CKJ16] Choi, Ben C.F.; Kim, Sung S.; Jiang, Zhenhui (Jack): Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior. Journal of Management Information Systems, 33(3):904–933, 2016.

[CMHD15] Casadesus-Masanell, Ramon; Hervas-Drane, Andres: Competing with Privacy. Management Science, 61(1):229–246, 2015.

[DH06] Dinev, Tamara; Hart, Paul: An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1):61–80, 2006.

[DM16] Dienlin, Tobias; Metzger, Miriam J.: An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample. Journal of Computer-Mediated Communication, 21(5):368–383, 2016.

[DT15] Dienlin, Tobias; Trepte, Sabine: Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3):285–297, 2015.

[Fe01] Feigenbaum, Joan; Freedman, Michael J; Sander, Tomas; Shostack, Adam: Privacy engineering for digital rights management systems. In: Digital Rights Management Workshop. Jgg. 2320. Springer, S. 76–105, 2001.

[GA07] Grossklags, Jens; Acquisti, Alessandro: When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. In: WEIS. 2007.

[GS67] Glaser, Barney G.; Strauss, Anselm L.: The Discovery of Grounded Theory. Aldine Pub., Chicago, 1967.

[Ha08] Hansen, Marit: Marrying Transparency Tools with User-Controlled Identity Management. In (Fischer-Hübner, S.; Duquenoy, P.; Zuccato, A.; Martucci, L., Hrsg.): The Future of Identity in the Information Society. IFIP — The International Federation for Information Processing, S. 199–220. Springer, Boston, MA, 2008.

[Hi10] Hirsch, Dennis D: The law and policy of online privacy: Regulation, self-regulation, or co-regulation. Seattle UL Rev., 34:439, 2010.

[Ho14] Hoffman, David: Privacy Is a Business Opportunity. Harvard Business Review, S. 2–5, 2014.

[Hu14] Hustinx, Peter: Preliminary Opinion of the European Data Protection Supervisor "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy". Bericht, European Data Protection Supervisor, March 2014. available via https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf.

[Li11] Liu, Zhan; Bonazzi, Riccardo; Fritscher, Boris; Pigneur, Yves: Privacy-friendly business models for location-based mobile services. Journal of Theoretical and Applied Electronic Commerce Research, 6(2):90–107, 2011.

[NHH07] Norberg, Patricia A.; Horne, Daniel R.; Horne, David A.: The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs, 41(1):100–126, jun 2007.

[Re16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Official Journal of the European Union, L 119/1, http://data.europa.eu/eli/reg/2016/679/oj, April 2016.

[Ro10] Rossnagel, Heiko: The Market Failure of Anonymity Services. In (Samarati, Pierangela; Tunstall, Michael; Posegga, Joachim; Markantonakis, Konstantinos; Sauveron, Damien, Hrsg.): Information Security Theory and Practices: Security and Privacy of Pervasive Systems and Smart Devices: 4th IFIP WG 11.2 International Workshop, WISTP 2010, Passau, Germany, April 12-14, 2010, Proceedings. Springer, 2010.

[Ru11] Rubinstein, Ira S: Regulating privacy by design. Berkeley Technology Law Journal, 26(3):1409–1456, 2011.

[SDX11] Smith, H. Jeff; Dinev, Tamara; Xu, Heng: Theory and Review Information Privacy Research: An Interdisciplinary Review. MIS Quarterly, 35(4):989–1015, 2011.

[SGB01] Spiekermann, Sarah; Grossklags, Jens; Berendt, Bettina: E-privacy in 2nd generation E-commerce. In: Proceedings of the 3rd ACM conference on Electronic Commerce - EC '01. ACM Press, New York, New York, USA, S. 38–47, oct 2001.

[St13] Strübing, Jörg: 1978. 2013.

[Te17] Technology Analysis Division of the Office of the Privacy Commissioner of Canada: Privacy Enhancing Technologies - A Review of Tools and Techniques. Bericht, Office of the Privacy Commissioner of Canada, November 2017. available via https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/.

[Xu12] Xu, Heng; Teo, Hock-Hai; Tan, Bernard CY; Agarwal, Ritu: Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. Information Systems Research, 23(4):1342–1363, 2012.

[Zi15] Zimmermann, Christian: A categorization of transparency-enhancing technologies. arXiv preprint arXiv:1507.04914, 2015.

All websites have been last accessed on December 5th, 2017.

A Demographische Daten der Interviewteilnehmer

Tab. 2: Demographische Daten der Interviewteilnehmer

Code	Branche	Unternehmensgröße Mitarbeiter	Unternehmensgröße Umsatz (in €)	Position	♂/♀	Dauer (hh:mm:ss)
A	Briefgesellschaft	1001-5000	50-100 Mio	Mitglied der Geschäftsleitung, Leiter Marketing und Vertrieb	♂	01:20:16
B	Zahlungssystem-Anbieter	51-200	n.a.	Produktionsmanager	♂	00:45:16
C	Energie-Beratung	11-50	1 Mio.	Geschäftsführer	♂	01:18:48
D	Anbieter E-Commerce-Lösungen	51-200	5-10 Mio.	Leiter Produktionsmanagement	♂	00:55:42
E	Anbieter E-Commerce-Lösungen	51-200	5-10 Mio.	Solutions Manager	♂	01:18:48
F	Anbieter E-Commerce-Lösungen	51-200	5-10 Mio.	Berater technische Pre-Sales	♂	00:44:57
G	Telekommunikation	0,1-0,5 Mio.	50-100 Mrd.	Experte Datenschutz-Audits und-Standards	♂	00:58:16
H	Telekommunikation	0,1-0,5 Mio.	50-100 Mrd.	Stellvertretender Leiter Datenschutz-Audits und-Standards	♂	00:58:16
I	Telekommunikation	0,1-0,5 Mio.	50-100 Mrd.	Leiter Datenschutz für Infrastrukturen und Dienstleistungen	♂	01:14:00
J	Beratung Technikfolgen-abschätzung IT	1-10	n.a.	Geschäftsführer	♂	01:51:26
K	Finanz-Dienstleister	50001-0,1 Mio.	20-50 Mrd.	Beraterin geschäftlicher Zahlungsverkehr	♀	01:49:48
L	Beratung IT-Management	1-10	n.a.	Geschäftsführer	♂	00:44:17