Schutz der Anonymität als Gemeinschaftsaufgabe – eine neue Generation von PETs?

Zbigniew Kwecka[1], William Buchanan[1], Burkhard Schafer[2], Judith Rauhofer[2]

[1]Napier University
School of Computing
Edinburgh
Edinburgh. EH10 5DT
z.kwecka@gmail.com
B.Buchanan@napier.ac.uk

[2]University of Edinburgh
School of Law
SCRIPT Centre for IT and IP Law
Old College, Edinburgh E8 9YL
B.schafer@ed.ac.uk
J.rauhofer@ed.ac.uk

Abstract: Dieser Aufsatz beschreibt einen neuen Zugang zu Privacy Enhancing Technologies, der seine rechtstheoretische Motivation aus einem Verständnis der Privatsphäre als kollektivem Gut gewinnt. In diesem Modell willigen alle Mitglieder einer Gruppe in ein theoretisches Risiko ein, um gegenseitig ihre Anonymität und damit einen wesentlichen Aspekt ihrer Privatsphäre zu sichern.

.

1 Einführung

Gegenstand dieses Aufsatzes ist ein neuer Ansatz zum Schutz der Anonymität von Verdächtigen im polizeilichen Ermittlungsverfahren und seine rechtlichen und rechtsphilosophischen Grundlagen. Wir stellen insbesondere ein neues Modell für Privacy Enhancing Technologies vor, das in Zusammenarbeit zwischen Informatikern der Napier University Edinburgh und des SCRIPT Zentrums an der juristischen Fakultät der University of Edinburgh entwickelt wurde. Diese interdisziplinäre und institutsübergreifende Zusammenarbeit wurde durch das Scottish Institute for Policing Research (SIPR) ermöglicht, und die resultierende „Investigative Data Acquisition Platform“ (IDAP) ist in erster Linie als ein Werkzeug gedacht, das der Polizei erlauben soll, im Ermittlungsverfahren zum einen die legitimen Datenschutzinteressen eines Verdächtigen besser zu schützen, andererseits aber auch die Interessen der Polizei an einer Geheimhaltung der Ermittlung zu gewährleisten. Dies verlangt eine neue

Perspektive auf die Rolle des Datenschutzes in der Gesellschaft allgemein, und im Ermittlungsverfahren im besonderen. Im ersten Teil dieser Arbeit entwickeln wir deshalb den rechtstheoretischen Rahmen unseres Ansatzes, und illustrieren die Grundgedanken anhand zweier kurzer Beispiele – je einem aus der Offline- und der Online-Welt. Obgleich der rechtliche Rahmen unserer Forschung seinen Schwerpunkt im britischen Recht hat, hoffen wir dass die rechtstheoretischen Grundlagen systemunabhängig Gültigkeit haben. Möglichkeiten der Anpassung der Software an andere rechtliche Rahmenbedingungen werden kurz diskutiert werden. Im zweiten Teil stellen wir die Bausteine und Architektur der IDAP dar, und diskutieren im dritten Teil abschließend wie durch Schaffung von rechtlichen, organisatorischen und institutionellen Rahmenbedingungen die notwendige gesellschaftliche Akzeptanz dieses Ansatzes erreicht werden kann.

2 „Ich bin Spartakus" - Privatsphäre und Gemeinschaftsinteresse

Traditionell wird der Schutz der Privatsphäre rechtlich als ein individuelles Schutzrecht konzipiert, das die Interessen des Einzelnen potentiell in Konflikt mit legitimen Gemeinschaftsinteressen, insbesondere dem Schutz der inneren Sicherheit und der Strafaufklärung, bringen kann. Dies ist selbst in der Etymologie des Wortes sichtbar: „Privat" ist vom lateinischen „privare" - rauben, unterschlagen – abgeleitet. „Privat" war der Römer dann, wenn er Staat und Gemeinschaft seiner Dienste beraubte, und seinen Freunden das Vergnügen seiner Gesellschaft vorenthielt. Der natürliche Zustand ist der des zoon politikon, das Leben im öffentlichen Raum. Ihm zu entkommen bedeutet, aktiv Schritte zu unternehmen und sich bewusst von anderen abzusondern. Im angelsächsischen Rechtskreis haben Louis Brandeis und Samuel D. Warren das Anrecht auf Privatsphäre als das *„right to be let alone",* das Recht allein gelassen zu werden, definiert. Es ist ein einsames, solitäres Recht, das logische Gegenstück zu den Rechten auf Versammlungs- und Vereinsfreiheit, den „sozialen" Rechten die nur gemeinschaftlich denkbar sind. Als Abwehrrecht gegen Übergriffe des Staates bleibt es dann sowohl prozedural-rechtlich wie auch technisch-praktisch dem Einzelnen überlassen, die effektive Durchsetzung dieses Rechts zu erreichen. Sollte ich entscheiden, meine Daten der Öffentlichkeit zugänglich zu machen, so verzichte ich auch durch meine autonome Handlung auf ihren Schutz vor den Augen Dritter. Wähle ich selbst öffentliche Medien um über mich selber zu sprechen – mein Blog oder Twitter – so wird jeder Anspruch auf Privatschutz aufgegeben.

Im amerikanischen Verfassungsrechts insbesondere entwickelte sich der Begriff der „reasonable expectation of privacy" als Voraussetzung des Privatheitsschutzes. Nur an bestimmten Orten kann ich sicher sein, dass mich das Recht vor den Augen anderer schützt. Paradigmatisch war dies das eigene Haus – my home is my castle – dessen physische Wände auch Schranken des Zugriffs auf Informationen über mich darstellen. Obgleich dieser Raumbezug später erweitert wurde (insbesondere in Katz v US Katz v. United States, 389 U.S. 347 (1967) blieb der Ansatz durch seine Betonung des subjektiven Schutzinteresses dem liberalen Privatheitsverständnis verhaftet. Effizienter Schutz der Privatsphäre heißt dann, dem Datensubjekt die Kontrolle über seine Daten zu geben, und ihm somit die Entscheidungsmöglichkeit zu lassen, wann und mit wem er

sich sicher genug fühlt, Informationen auszutauschen und den engsten Schutzbereich zu verlassen. In der digitalen Welt finden wir den analogen Gedanken etwa bei den Standardeinstellung auf Facebook. Die normale Einstellung ist die Bereitschaft Informationen zu teilen. Wenn ich dies nicht will, kann ich durch meine eigene Entscheidung die Einstellung so ändern, dass anderen Zugriff verwehrt wird. Ich allein schütze meine Privatsphäre, und ich schütze sie dadurch, dass ich andere ausgrenze. Wikipedia veranschaulicht diesen Gedenken visuell sehr effizient durch ein Bild, in dem die Außenwelt durch eine Kette abgewehrt wird, und der Eigentümer gleichzeitig durch ein Schriftzeichen seine Absicht kundtut, dass er in Ruhe gelassen werden will. Privacy Enhancing Technologies haben in der Vergangenheit diesem juristischen und gesellschaftlichen Verständnis des Privatschutzes entsprochen. Die Wände des Hauses werden die Firewall; Verschlüsselungstechnologien geben mir die Möglichkeit, zu entscheiden, welche Informationen Dritte nicht sehen können, Anonymisierungsverfahren halten Daten von möglichen Überwachern fern. Datensparsamkeit und Datenvermeidung werden zentrale Vorgaben zum Schutz der Privatsphäre. Je weniger Informationen ich in die Welt lasse, desto geschützter ist meine Privatsphäre.

Es gibt aber auch eine ganz andere Art, über die Privatsphäre nachzudenken. Hier ist sie nicht Zeichen einer selbstsüchtigen Abgeschiedenheit von der Gesellschaft, sondern vorausbedingt für soziale Güter, insbesondere Teilnahme am demokratischen Prozess und der öffentlichen Meinungsbildung. Privatheitsschutz erlaubt es Bürgern, Maßnahmen der Regierung zu kritisieren und sich ihnen zu widersetzen, insbesondere wenn diese Maßnahmen undemokratisch oder totalitär sind. Privatheitsschutz erlaubt es, sich dem Druck gesellschaftlicher Erwartungshaltungen zu widersetzen, die sonst eine Gefahr für Individualität und Menschenwürde werden können, und damit auch für den Freiheitsbegriff, der auf diesen beruht. Solch ein Verständnis der Bedeutung der Privatsphäre hat in den letzten Jahren auch gerade durch den Einfluss neuer Technologien immer mehr Vertreter gewonnen. So argumentierte etwa Bloustein [Bl1964 S. 1003] dass:

"[t]he man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man."

Ähnlich argumentiert Simitis [Si1984 S.399], dass der Konflikt zwischen den „demokratischen Rechten" auf Redefreiheit und Transparenz mit dem Schutz der Privatsphäre oft auf einem Missverständnis beruht, und dass ganz im Gegenteil auch die Privatsphäre eine wichtige Rolle darin spielt, Teilnahme am öffentlichen Leben zu erleichtern. In der Tat zeigt die Erfahrung mit totalitären Systemen, dass die systematische Verletzung der Privatsphäe oft zu einer „Gesellschaft der Mitläufer" führen kann.

Die gegenseitige Abhängigkeit zwischen Schutz der Privatsphäre und Schutz anderer zentraler Charakteristiken der offenen, pluralistischen Demokratie wird auch von Charles Raab (2012) hervorgehoben, der argumentiert, dass Werte wie persönliche Autonomie, Privatsphäre und informationelle Selbstbestimmung

"are important not primarily because individuals may wish to live in isolation (for they do not, mostly), but so that they can participate in social and political relationships at various levels of scale, and so that they can undertake projects and pursue their own goals".

Wenn diese Analyse aber Gültigkeit besitzt, und die Privatsphäre damit ein kollektives Gut darstellt, so sollte auch ihr Schutz und ihre Durchsetzung nicht nur dem Einzelnen überlassen werden. Dieser Gedanke hat zwei Konsequenzen: Zum einen kann es bedeuten, dass der Einzelne nicht immer das Recht hat, seine Privatheit aufzugeben. Autonomie findet ihre Schranken im Gemeininteresse. So argumentiert etwa Regan [Re1995 S. 233]

"[i]f one individual or a group of individuals waives privacy rights, the level of privacy for all individuals decreases because the value of privacy [in the collective view of society] decreases"

Sich für „Big Brother" freiwillig zu melden, so dieses Argument, schadet nicht nur dem Partizipanten, es schadet der Gesellschaft, da es Privatheit entwertet. Wir werden später zu dieser Idee zurückkommen müssen, da der Gedanke, dass es kein uneingeschränktes Recht darauf gibt, seine Privatsphäre aufzugeben, für unseren technologischen Ansatz ein potentielles Problem darstellen könnte.

Auf der anderen Seite bedeutet dies aber auch, dass ich als Bürger die Solidarität meiner Mitbürger einfordern darf, wenn meine Privatsphäre unrechtmäßig bedroht ist. Was dies bedeuten kann, wird in besonders anschaulicher Weise in Stanley Kubricks Film „Spartakus" aus dem Jahr 1960 sichtbar. Nach dem Sieg des römischen Heers über die von Spartakus geleiteten Sklaven will General Crassus Spartakus festnehmen. Er verspricht den Unterlegenen das Leben, wenn sie ihm ihren Führer ausliefern, ansonsten droht ihnen der Tod. Spartakus, um ihnen dieses Schicksal zu ersparen, tritt vor und bekennt: *„Ich bin Spartakus"*. Seine Gefährten aber lehnen dies Opfer ab. Einer nach dem anderen tritt vor und behauptet: Ich bin Spartacus!, bis die Kakophonie der Stimmen die der Römer übertönt. Crassus ist in seinem Versuch, Spartakus zu identifizieren, gescheitert. Hier sehen wir wie ein Verständnis von Anonymität als Gemeinschaftsaufgabe auch den Gedanken, dass Privatheitsschutz Datensparsamkeit und Datenvermeidung bedeutet, in Frage stellen oder zumindest modifizieren kann. In unserem Beispiel ist es gerade die Überflutung mit „Lärm" (im Englischen „white noise" in Anlehnung an das Rauschen eines schlecht eingestellten Radiosenders), die es dem unterdrückenden Staat unmöglich macht, sein Ziel zu identifizieren. Datensparsamkeit bleibt zwar „globales" Ziel, das heisst es sollen nur so wenig „echte" und „Verschleierungsdaten" wie absolut nötig erhoben werden, um das Ziel einer sichern Datenerhebung zu ermöglichen, auch wenn dies „lokal", das heisst für den Verschleierer, erst einmal ein mehr an Daten bedeutet.

Damit haben wir die rechtsphilosophischen Grundlagen für unsere Neuorientierung gelegt: wenn Firewallls, Verschlüsselung und Datensparsamkeit PETS sind, die dem

Leitbild der Privatheit als Individualrecht folgen, wie können PETs aussehen, die für die Gemeinschaft das leistet, was im Film die Sklaven für Spartakus tun? Und gibt es Anwendungen, die denen im Film entsprechen und für die daher dieser Ansatz besonders geeignet ist? Im nächsten Abschnitt stellen wir ein Anwendungsbeispiel vor, das wichtige strukturelle Gemeinsamkeiten mit Spartakus' Dilemma hat, um dann im abschließenden Teil eine technologische Lösung zu diskutieren.

3. Anwendungsbeispiel: Polizeiliche Ermittlung und Schutz der Anonymität

Max Mustermann wird von der Polizei des Kindesmissbrauchs verdächtigt. Insbesondere vermutet die Polizei, dass er regelmäßig minderjährige Prostituierte in seine Wohnung einlädt. Um diesen Anfangsverdacht zu bestätigen, fährt die Polizei in seiner Nachbarschaft mit einem Streifenwagen vor, und uniformierte Beamte führen Hausbefragungen durch. Sollten sie die Nachbarn fragen, ob diese „spät in der Nacht Kinder ins Haus des Mustermanns haben gehen sehen“, ergeben sich zwei offensichtliche Risiken. Zum einen gibt es das offensichtliche Risiko für Mustermann, näseine Reputation und sein Ansehen in der Gemeinschaft. Die Nachbarn wissen nun, dass er von der Polizei verdächtigt wird, und können wahrscheinlich auch Rückschlüsse über die angebliche Straftat schließen. Sie können damit indirekt Information über die Daten erschließen, die die Polizei wohl über Mustermann besitzt, und wenn sie wie so viele glauben, dass Rauch auch Feuer bedeutet, könnten auf Grund dieser Information informelle Sanktionen gegen Mustermann beginnen. So dieser unschuldig ist, würde ihm damit ein schweres Unrecht getan. Gleichzeitig setzt sich aber auch die Polizei einem Risiko aus - was wenn die Nachbarn, absichtlich oder versehentlich, Mustermann über das Interesse der Polizei in seine Person informieren? So dieser schuldig ist, könnte er die Flucht ergreifen, oder Beweismittel vernichten. Es ist deshalb für beide Seiten besser, wenn die Identität von Mustermann gegenüber seinen Nachbarn geheim gehalten wird, und seine Anonymität geschützt wird. Dies kann zum Beispiel dadurch geschehen, dass sehr weite und allgemeine Fragen gestellt werden, und die Polizei nicht nur am Haus der Nachbarn klopft, sondern auch an dem von Mustermann selber. Nicht also: „Haben Sie Minderjährige im Haus ihres Nachbarn Mustermann gesehen“, sondern „Haben Sie in letzter Zeit häufiger junge Menschen in der Nachbarschaft spät am Abend gesehen, die hier nicht normalerweise wohnen?“ Dies erzeugt mehr Daten, und erschwert es, die relevante Information herauszufinden, doch ist es gerade dieses Mehr an Daten, das die Anonymität von Mustermann schützt. Natürlich gilt es hier eine Balance zu wahren – wenn die Fragen zu vage werden („Haben Sie irgendetwas Ungewöhnliches gesehen?“) bewegt sich der Nutzen der Antworten gegen Null. Wir halten jedoch eine derartige Vorgehensweise der Polizei in traditionellen Ermittlungsverfahren weder für ethisch noch rechtlich bedenklich, auch wenn sie dadurch als Beiprodukt Informationen erlangen, die mit dem eigentlichen Ziel der Ermittlung wenig zu tun haben werden.

Im Online-Ermittlungsverfahren sieht die Situation dagegen anders aus. Spätestens seit den Terroranschlägen in 2001 haben die meisten Regierungen weitreichende

Verpflichtungen zur Datenspeicherung, insbesondere für ISPs und andere Telekommunikationsanbieter geschaffen [SS02] [Yo06]. Gleichfalls wurde der Zugriff der Polizei auf diese Daten gesetzlich geregelt, in Großbritannien etwa durch den „Regulation of Investigatory Powers Act (RIPA)“. Um eine bessere Balance zwischen dem Interesse des Staates an effizienter Strafverfolgung und dem Interesse des Bürgers auf Schutz seiner Privatsphäre zu gewährleisten, muss ein formales Verfahren eingehalten werden, bei dem die Polizei einen ausreichenden Anfangsverdacht und ausreichend klare Beschreibung der verlangten Information angeben muss. Dies soll unzulässige Rasterfahndungen unterbinden und so den Privatheitsschutz stärken. Wie unser Fallbeispiel aber zeigt wird die Polizei damit aber auch paradoxerweise verpflichtet, dem Datenbesitzer die Identität des Verdächtigen offenzulegen. Wir können uns nun leicht Situationen vorstellen, in denen dies ebenso problematisch ist wie in unserem Offline Beispiel. Wenn Google gezwungen wird, der Polizei meine Identität und Adresse zu übermitteln, da diese glaubt, mein Blog enthalte illegales Material, könnte Google in Versuchung geführt sein, mein Konto mit ihnen zu schließen, um Reputationsschaden zu vermeiden. Gleichfalls möchte ich wahrscheinlich auch nicht, dass meine Bank von einem wie auch immer gearteten Interesse der Polizei in meine Person erfährt, wenn ich mit ihr gerade über die Verlängerung meines Kredits verhandle. Andererseits würden mich jegliche Sanktionen unter Umständen vorzeitig vor der Untersuchung der Polizei warnen. Da es aus rechtlichen Gründen für die Polizei unmöglich ist, meine Identität durch geschicktes Fragen zu verschleiern, simuliert unsere Plattform, die wir im nächsten Abschnitt vorstellen, die Verschleierung von Identitäten durch kollektives Handeln, so wie auch in Spartakus die Identität des Anführers durch kollektives Handeln verschleiert wurde.

4. Die IDAP Plattform

4.1 Informelle Beschreibung

Der Grundgedanke hinter der IDAP ist wie gesagt die Verschleierung von Identität durch kollektives Handeln. Informell kann ihr Verhalten so beschrieben werden: Die Polizei fragt zum Beispiel den ISP oder die Bank nicht direkt nach den Daten von Herrn Mustermann. Stadtdessen generiert die Anfrage durch einen Zufallsalgorithmus eine ganze Liste von Personen (je länger die Liste, desto besser der Schutz). Die Bank weiß nur, dass irgendeine der Personen auf dieser Liste das Interesse der Polizei erregt hat – da sie aber auch weiß, dass die anderen Namen durch einen Zufallsalgorithmus erzeugt wurden, sagt ihr diese Information wenig. Insbesondere kann sie keine Sanktionen gegen jeden Name auf der Liste ergreifen. Die Gesamtheit dieser Daten erreicht die Polizei aber nur in stark verschlüsselter Form. Sie hat einen Schlüssel, der aber nur die Daten des Verdächtigen entschlüsseln kann, der Rest der Information, der Lärm der nur erzeugt wurde um gegenüber der Bank die Identität des Verdächtigen zu verschleiern, ist für sie unlesbar.

Wir könnten das öffentliche Vertrauen in diesen Vorgang noch dadurch verstärken, dass wir institutionell einen "vertrauenswürdigen Dritten", etwa eine Datenschutzbehörde, mit einbeziehen. In diesem Fall werden die gesamten Daten diesem Drittanbieter übermittelt,

der dann die Aufgabe übernimmt, alle überflüssigen Daten zu vernichten, und nur die des Verdächtigen an die Polizei weiterzuleiten. Anders als die Bank oder der ISP hat diese dritte Partei kein direktes, persönliches Interesse an der Identität des Verdächtigen. Dass sie (notwendigerweise) in der Lage wäre, diese festzustellen, ist deshalb mit weniger Risiko verbunden. Gleichfalls hat sie, anders als die Polizei, aber auch kein Interesse daran, die überflüssigen Daten zu speichern, in der Hoffnung, dass irgendwann Fortentwicklungen der Technologie ihr doch Zugang ermöglichen könnten.

4.2 IDAP Bausteine

Informationsgewinnung von einer dritten Partei, die Privatheit schützt, ist ein bekanntes Problem. Was wir suchen, legt vieles über uns offen – das ist z.B. das Geschäftsmodell von Google. Private Information Retrieval (PIR) Protokolle waren ursprünglich so entwickelt worden, dass der Sender nicht feststellen kann, an welcher Information der Chooser, der die Anfrage stellt, interessiert ist. Sie waren allerdings nicht an der Geheimhaltung der Ursprungsdaten selbst interessiert, so dass im Extremfall dieses Ergebnis dadurch erzielt werden kann, dass die gesamte Datenbank an den Chooser übermittelt wird. Als sehr einfaches Beispiel können wir uns vorstellen, dass eine online Apotheke einen Katalog mit ihren Produkten im Internet bereitstellt. Wenn ich nicht will, dass die Apotheke sieht, an welchen Produkten ich interessiert bin, bevor ich bereit bin sie zu kaufen, ist es besser für mich, den Katalog in pdf auf meinem Computer zu speichern als die html Version online zu benutzen, die der Apotheke zeigt auf welchen Seiten ich besonders lange geblieben bin. Da diese Daten aber sowieso öffentlich sind, gibt es von der Seite der Apotheke keine Bedenken, sie mir alle zugänglich zu machen.

Die Hauptmotivation hinter diesen PIR Schemata ist daher minimale Komplexität der Kommunikation und der Rechnerleistung [OS07]. Interessanter sind Anwendungen, in denen auch der Chooser bestimmte Informationen nicht sehen können soll. Der dazu nötige striktere Ansatz als PIR ist 1-out-of-n Oblivious Transfer (OT) primitive, der es ermöglicht, einen zufällig gewählten Eintrag aus einem Datensatz mit n Einträgen im Besitz des Senders so herauszugreifen, dass der Sender nicht herausfinden kann, welcher Eintrag übermittelt wurde, der Chooser aber nichts über die anderen Einträge in dem Datensatz erfahren kann [Sc95]. 1-out-of-n OT Protokolle, die es dem Chooser ermöglichen, aktiv einen Eintrag auszuwählen, und die lineare oder sub-lineare Komplexität haben, werden als symmetrische PIR (SPIR) Protokolle bezeichnet. Diese nützlichen privatheitschützenden Informationsgewinnungsprotokolle haben in einer Reihe von Systemen Anwendung gefunden, etwa elektronische Listen von gestohlenen Kreditkarten [FA03]; kooperative wissenschaftliche Datenverarbeitung [DA01], [GL02); und online Auktionen [Ca99].

Mit diesen Protokollen kann der Chooser vertraulich einen Eintrag aus der Datenbank des Senders extrahieren, wobei er allerdings zuerst verdeckt auf den Index in der Datenbank des Senders zurückgreifen muss. In SPIR Anwendungen wird vorausgesetzt, dass solch ein Index öffentlich zugänglich ist [AIR01]; [BD01] – eine Situation die aber in den meisten Ermittlungsverfahren nicht gegeben sein wird. Zudem wird der Ermittler in der Regel auf den Verdächtigen durch einen Namen, Telefonnummer oder auch nur eine Beschreibung Bezug nehmen wollen. Bevor die Daten daher durch SIPR extrahiert

werden können, muss der Chooser eine vertrauliche Suche in der Datenbank des Senders machen können. Protokolle, die diesen vertraulichen Vergleich der Werte ermöglichen, werden Private Equality Test (PEqT) Protokolle genannt. Sie verwenden in der Regel kommutative [FA03];[Kw08] oder homomorphische Verschlüsselungssysteme [BD01]. Wir können nun die Private Equijoin Protokolle beschreiben, die das Herz von IDAP sind.

Viele Kryptographiesysteme verwenden sequentielle Verschlüsselung und Entschlüsselung, da die sequentielle Anwendung verschiedener Systeme das Ergebnis verstärkt [Sh49]; [We06]. Eine besonderer Klasse dieser sequentiellen Kryptographiesysteme – kommutative Kryptographiesysteme – erlauben die Entschlüsselung eines Textes in willkürlicher Ordnung. Die Vorteile solch eines Systems wurden von Shamir [Sh80] hervorgehoben, der es in dem klassischen Spiel Mental Poker verwendete, das er zusammen mit Rivest and Aldman entwickelte. In diesem Spiel verwenden sie ein Three-Pass (3Pass) geheimes Austauschprotokoll. Das am weitesten verbreitete kommutative Kryptographiesystem basiert auf Pohling-Hellmans (PH), asymmetrisch privatem Schlüssel [PH78]. Die größte Stärke dieses Asatzes ist, dass es für Schlüssel, die auf der gleichen Primzahl beruhen, kommutativ ist, und daher den Vergleich verschlüsselter Chiffretexte erlaubt. Dank dieser Eigenschaften kann es für ein 3Pass primitive verwendet werden, dass es den Parteien erlaubt, Dateien ohne Schlüssel zu versenden und trotzdem PEqT durchzuführen, das privaten Abgleich von Einträgen erlaubt.

Das 3Pass Protokoll erlaubt zwei Parteien ein Geheimnis zu teilen, ohne private oder öffentliche Schlüssel auszutauschen. Ein physisches Gegenstück ist das folgende Beispiel.

1. Alice legt eine geheime Botschaft m in eine Truhe, und verschließt sie mit einem Vorhängeschloss.
2. Die Truhe wird an Bob gesendet, der sein eigenes Vorhängeschloss hinzufügt und die Truhe zurücksendet.
3. Alice entfernt ihr Schloss, und sendet die Truhe zurück an Bob.
4. Bob entfernt sein Schloss, und kann nun die Nachricht in der Truhe lesen.

Zusätzliche Parteien oder Verschlüsselungsstufen (die Vorhängeschlösser) können hinzugefügt werden, so dass ein Klartext mehrfach verschlüsselt werden kann, solange alle Parteien kooperieren. Es ist diese Funktionalität die wir für IDAP brauchen.

PEqT Protokolle können dazu verwendet werden, um privat zu verifizieren, ob 2 geheime Eingaben identisch sind. Agrawal, Evfimievski and Srikant (2003) entwickelten ein besonders flexibles PEqT Protokoll, das in den folgenden Stufen beschrieben werden kann:

1. Alice verschlüsselt ihre Eingabe und sendet sie an Bob.

2. Bob verschlüsselt den Chiffretext, den er von Alice erhalten hat, und sendet ihn zurück.

3. Bob verschlüsselt seine geheime Eingabe und sendet sie an Alice.

4. Alice verschlüsselt den Chiffretext mit Bobs Eingabe.

5. Alice vergleicht die beiden resultierenden Chiffretexte – sind sie identisch, so waren die Eingaben identisch.

6. Alice kann Bob das Ergebnis mitteilen, oder es geheim halten.

Wenn wir nun PEqT and 3Pass primitives verbinden, erhalten wir ein „Private Equijoin" Protokoll, das die Grundlage von IDAP bildet. Ein Private Equijoin oder PE Protokol erlaube es zwei Parteien, dem Chooser und dem Sender, privat ihre Datensätze bezüglich der Werte V_C and V_S zu vergleichen, und erlaubt es dem Chooser gewisse zusätzliche Informationen über V_C bezüglich eines gegebenen Parameters zu erlangen.

Der Ablauf des Datenaustausches ist hier kurz illustriert

1. Beide Parteien verschlüsseln mit der hash Funktion h die Elemente in ihren Mengen, so dass $X_C = h(V_C)$ and $X_S = h(V_S)$. Chooser wählt einen geheimen PH Schlüssel E_C zufällig aus, und Sender wählt zwei PH Schlüssel E_S and E'_S, alle aus der gleichen Gruppe Z^*_p.

2. Chooser verschlüsselt die Einträge in ihrer Menge: $Y_C = E_C(X_C) = E_C(h(V_C))$.

3. Chooser sendet dem Sender die Menge Y_C, lexikographisch geordnet.

4. Sender dechiffriert jeden Eintrag $y \in Y_C$, den er vom Chooser bekommt, sowohl mit E_S und E'_S, und sendet für jeden ein 3-tuple $\langle y, E_S(y), E'_S(y) \rangle$ zurück

5. Für jedes $h(v) \in X_S$, tut der Sender das Folgende:

(a) Verschlüsselt $h(v)$ mit E_S für den equality test.

(b) Verschlüselt $h(v)$ mit E'_S zum Schutz der zusätzliche Information über v, $\kappa(v) = E'_S(h(v))$.

(c) Verschlüsselt die zusätzliche Information $ext(v)$:

$c(v) = K(\kappa(v), ext(v))$

Wobei K eine symmetrische Verschlüsselungsfunktion ist, und $\kappa(v)$ der im Schritt 5b hergestellte Schlüssel ist.

(d) Erstellt ein Paar $\langle E_S(h(v)), c(v)\rangle$. Diese Paare, von denen jedes ein privat abgeglichenes Element und die verschlüsselte Zusatzinformation über den Eintrag v enthält, werden dann dem Chooser übermittelt.

6. Chooser entfernt ihre Verschlüsselung E_C von allen Eintragungen in den 3-Tupeln die sie im Schritt 4 erhalten hat, und erzeugt so Tupel α, β, und γ so dass $\langle \alpha, \beta, \gamma\rangle = \langle h(v), E_S(h(v)), E'_S(h(v))\rangle$. Somit ist α der gehashte Wert $v \in V_C$, β ist der gehashte Wert v durch E_S verschlüsselt, und γ ist der gehashte Wert v der mit E'_S verschlüsselt ist.

7. Chooser ignoriert alle Paare die sie in Schritt 5 erhalten hat, wenn deren erster Wert denen der β Tupeln entspricht, die sie im Schritt 6 erzeugt hat. Dann verwendet sie die γ Tupel als symmetrische Schlüssel um die zusätzliche Information im zweiten Eintrag des Paares $\langle E_S(h(v)), c(v)\rangle$ zu entschlüsseln.

Damit haben wir das Skelett unseres Ansatzes beschrieben. Chooser, in unserem Beispielfall die Polizei, und Sender, etwa die Bank oder der ISP des Verdächtigen, tauschen Dechiffrierschlüssel aus. Chooser verlangt dann vom Sender eine ganze Reihe von Dokumenten, sowohl die des Verdächtigen als auch eine Reihe von anderen, durch Zufallsgenerator ausgewählt, die die alleinige Aufgabe haben die Identität des Verdächtigen vor dem Sender zu verschleiern. Diese Gruppe von Dokumenten wird so ausgewählt, dass Chooser zwar sicher sein kann, dass sich die gewünschte Information darunter befindet, aber ohne Kontrolle darüber, welche anderen Dokumente als „Schleier“ mit ausgewählt wurden. Der Sender wiederum kann nicht wissen, welche der vielen Personen zu denen von ihm Daten verlangt wurden der Verdächtige ist, und welche bloß zur Verschleierung dienen. Er kann trotzdem die Daten so verschlüsseln, dass der Chooser nur diejenigen wieder entschlüsseln kann, die zu dem bestimmten Verdächtigen gehören. Dieser Datensatz wird dann an den Chooser übermittelt. Dieser entschlüsselt daraufhin die und nur die Daten, die sich auf den Verdächtigen beziehen, für die anderen besitzt er keinen geeigneten Schlüssel. Idealerweise sollte es dann ein Verfahren geben, in dem er nachweislich die für ihn unnötigen und unlesbaren Daten sicher und prüffähig vernichtet.

5. Juristische Evaluierung und offene Fragen

Das System, das wir in diesem Aufsatz beschrieben haben, und seine Erweiterungen und Verfeinerungen, die wir anderenorts dargestellt haben, implementieren den abstrakten Gedanken des Technologie-unterstützten Privatheitsschutz als Gemeinschaftsaufgabe. Getreu dem Gedanken der „Share Economy“ (oder Shareconomy) nach der sich der

Wohlstand aller erhöht, je mehr alle Marktteilnehmern miteinander teilen [We984], wird hier die Sicherheit für alle erhöht, je mehr sie bereit sind, Daten und damit ihr Privatheitsrisiko zu teilen.

Unser Ansatz erlaubt es, das Risiko, dem sich der Verdächtige ausgesetzt sieht, und das Risiko der „Verschleierer", in verschiedener Weise im Einzelfall gegeneinander abzuwägen. Dies geschieht durch die formale Definition eines „Verschleierungsfaktors" o, den wir in [Kw09] vorgestellt haben. Intuitiv ist die Sicherheit für den Verdächtigen umso höher, je mehr Dokumente von Dritten verlangt werden. Das abstrakte Risiko dieser Dritten erhöht sich natürlich, je mehr von ihnen benötigt werden. Wenn in einer Datenbank von 1m Klienten bei jeder polizeilichen Nachfrage nur 10 als Verschleierung benötigt werden, ist mein persönliches Risiko, je zur Verschleierung herangezogen zu werden statistisch sehr gering. Sollten dagegen in einer Datenbank von nur 1000 Klienten jedes mal 100 als Verschleierung benötigt werden, so ist für mich die Wahrscheinlichkeit, dass meine Daten sogar mehrmals verwendet werden sehr hoch, und damit auch das Risiko dass ich in einem von diesen Fällen durch einen, wie auch immer unwahrscheinlichen, Fehler meine Identität offen gelegt wird. Der Verschleierunsgfaktors o erlaubt uns dieses abstrakte Risiko zu definieren, und in angemessener Weise zu variieren. Die Natur der Information spielt dabei eine weitere wichtige Rolle. Nehmen wir an, Mustermann ist wieder einmal des Kindesmissbrauchs verdächtigt. Als Teil ihres Falles möchte die Polizei dafür Beweise erbringen, dass er in der Tat ein ungesundes Interesse an Minderjährigen zeigt, insbesondere dass er als alleinstehender Mann, eine große Zahl von Katalogen mit Kinderunterwäsche bestellt hat. Die Information „hat Kinderwäschekatalog bestellt" ist nur im Rahmen einer Ermittlung, in der es bereits andere starke Verdachtsmomente gibt inkriminierend. In Isolierung ist er völlig harmlos, und eine Großzahl der „Verschleierung" wird in diesem Fall von jungen Familien kommen, die natürlich Kataloge dieser Art bestellen. Andererseits ist wegen der Schwere des Vorwurfs das Risiko für Mustermann, als Pädophiler verdächtigt zu werden, besonders hoch. In diesem Fall sollten daher viele „Verschleierer" gebraucht werden. Selbst in dem extrem unwahrscheinlichen Fall, dass die Daten dieser Dritten rechtswidrig entschlüsselt würden, würde nichts Wichtiges über sie preisgegeben. Anders ist die Situation, in der die Polizei zeigen will, dass Mustermann Viagra eingenommen hat, bevor er eine Sexualstraftat beging, und von einer online Apotheke herausfinden will, ob er in der relevanten Zeit Viagra bestellt hat. Hier könnte die Information „hat Viagra bestellt" auch für unsere Dritten peinlich sein, und dies unabhängig von irgend einer Ermittlungshypothese. Einem jungen Paar wird es egal sein können, dass sein Interesse an Kinderkleidung bekannt wird, er hingegen wird es nicht unbedingt gerne sehen, wenn ein Polizist, der ja auch sein Nachbar sein kann, liest dass er Viagra genommen hat. In dieser Situation werden wir (trotz Verschlüsselung) die Zahl der „Tarndokumente„ so klein wie Möglich halten, um selbst das abstrakte Risiko zu minimieren.

Unabhängig von der technischen Realisierung eröffnet dieser Ansatz eine Reihe von interessanten Fragen an Rechtsdogmatik, Rechtstheorie, Ethik und Sozialwissenschaften. Sind zum Beispiel die verschlüsselten Daten der Dritten, die ja ausschließlich der Verschleierung dienen, noch „personenbezogene Daten" im Sinne des Datenschutzrechts? Sie sind stark verschlüsselt, so dass formal beweisbar nur noch ein

abstraktes Risiko (etwa ein zukünftiger wissenschaftlicher Durchbruch) besteht, dass sie gelesen werden können. Da der Sender zudem keinen Bedarf oder Interesse an dem Schlüssel für die Verschleierungsdaten hat, kann dieser sofort nach Gebrauch gelöscht werden, so dass noch nicht einmal die theoretische Möglichkeit bestünde, durch Kombination von Information von Sender und Chooser die Identität des Datensubjekts zu erlangen.

Wir selber ziehen trotz allem die Interpretation vor, nach der auch ein abstraktes Risiko ausreicht, datenschutzrechtliche Vorschriften zum Greifen zu bringen. In diesem Fall bedarf ihre Verarbeitung einen der sechs in der Richtline aufgeführten Gründe. Sollten das Argument im ersten Teil unseres Aufsatzes, das Schutz der Anonymität als Gemeinschaftsgut Voraussetzung für den demokratischen Staat ist überzeugend sein, so könnte dies unter Umständen die „Verarbeitung im lebensnotwendigen Interesse des Betroffenen“ sein – auch wenn für den Verschleierer dieses Interesse nur indirekt gilt, um in der Zukunft selber den gleichen Schutz zu geniessen. Wahrscheinlich besser ist das Argument, dass die Verarbeitung zur Erfüllung einer Aufgabe im öffentlichen Interesse oder in Ausübung einer öffentlich-rechtlichen Funktion notwendig ist. Teilnahme an einem Schema der gegenseitigen Unterstützung wäre dann Bürgerpflicht, das rein abstrakte Risiko das durch die Preisgabe der eigenen Daten besteht eine Art „Privatheitssteuer“.

Aus Platzgründen können wir nicht alle Rechtsgrundlagen eingehend behandeln, und werden uns im Folgenden auf eine dritte Rechtsgrundlage, die der Einwilligung des Datensubjekts, konzentrieren. Dies erlaubt uns, einige der technischen und philosophischen Themen weiter auszuführen. Einwilligung wirft etwa die Fragen auf: wie viel müssen die Datensubjekte über ihr Risiko verstehen, damit ihre Einwilligung Gehalt hat? Und was für eine Art von Anreizen wäre rechtlich zulässig, wirtschaftlich effizient und psychologisch wirksam um dieses Risiko akzeptable zu machen?

Was ist also das Risiko im schlimmsten Fall? Im schlimmsten Fall könnte die Polizei die durch einen Zufallsgenerator ausgewählten Daten der dritten Parteien nicht, wie vorgeschrieben, sofort vernichten, sondern insgeheim speichern. Sie müsste dann in hochmoderne und leistungsstarke Entschlüsselungstechnologien investieren, um diese Daten vielleicht in der Zukunft dechiffrieren zu können. Selbst dann aber wären die Daten, die sie dadurch erhält, nichts mehr als willkürliche Schnappschüsse, ohne Kontext und sinnvolle Gemeinsamkeiten. In unserem Beispiel könnte sie etwa lernen, dass vor einiger Zeit Lisa Müller einen Wäschekatalog bestellt hat, oder Anton Schmidt Viagra kaufte, obwohl sie eigentlich nur an Herrn Mustermann interessiert hätten sein dürfen. Es gibt für sie in unserem Ansatz aber keine Möglichkeit, gezielt Daten über Dritte mit voraussehbarem Inhalt zu bekommen.

Um auch noch das theoretische Restrisiko weiter zu verringern und die gesellschaftliche Akzeptanz zu erhöhen, könnte dieser Ansatz leicht mit einer „trusted third party“ erweitert werden, die dann wiederum von den Datenschutzbehörden kontroliiert wird. In diesem Modell fungiert die TTP als proxy zwischen Sender und Chooser, so dass

1. Jede Kommunikation zwischen chooser und sender geht über die proxy.

2. Chooser übergibt proxy die Identifizierungsmerkmale der relevanten Dateneinträge, die von sender verschlüsselt wurden. Dies geschieht über eine sichere Verbindung und mit einem 3Pass Protokol.

3. Wenn nun von Sender im Schritt C4 Daten transferiert werden, so filtert proxy von diesen alle Dokumente aus, die nicht von Chooser verlangt werden, und nur der Verschleierung dienen. Diese werden dann vernichtet.

Voraussetzung für diesen Ansatz ist, dass die trusted third party selber kein Interesse an der Identität des Verdächtigen hat, und gleichfalls kein Interesse, die wahllos zur Verschleierung herausgegriffenen Daten Dritter nicht nur zu speichern, sondern dann stark in hochmoderne und leistungsstarke Entschlüsselungstechnologien zu investieren, um diese zu entschlüsseln. Anders als die Polizei hat sie nicht einmal ein abstraktes Interesse, oder die abstrakte Fähigkeit, die rechtlichen Vorschriften zu umgehen. Gleichfalls hat sie aber anders als der ISP oder die Bank auch kein Eigeninteresse, die Identität des Verdächtigen herauszufinden und dieses Wissen gegen ihn verwenden zu können.

Trotz dieser Maßnahmen könnten natürlich viele Kunden entscheiden, an einem solchen Schema gegenseitigen Identitätsschutzes nicht teilnehmen zu wollen. Dies kann schnell zum Zusammenbruch des Systems führen, dass letztendlich auf einer Form der „Herdenimmunität“ beruht [Fi93]. So wie Krankheiten schnell Verbreitung finden können, wenn die Rate der Impfgeschützen zu gering wird, so kann die Identität des Verdächtigen leicht entdeckt werden, wenn zu wenige andere Klienten bereit sind, ihre Daten zur Verschleierung zur Verfügung zu stellen. Aus der Forschung in soziale Netzwerke wissen wir zudem, dass hier Herdenimmunität besonders bruchgefährdet ist, da die Populationen typischerweise nicht so heterogen wie die Gesamtbevölkerung sind [Fe10]. Für virtuelle soziale Netzwerke wie Facebook oder eine Usenet Newsgroup, die sonst ein typisches Anwendungsbeispiel unseres Ansatzes sein könnten, ist dies deshalb besonders problematisch. Aus diesem Grund machen einige Staate im Bereich der Medizin die Impfung verpflichtend – das Gemeininteresse an Gesundheit überwiegt hier gegenüber dem abstrakten Risiko des Einzelnen, einen Impfschaden zu erleiden. Wie oben ausgeführt sind unsere Wurzeln des Daten- und Privatschutzes zu sehr dem liberalen Ethos des Individualrechts verbunden, um das medizinische Argument problemlos analog anwenden zu können, und wir haben bereits argumentiert, dass freiwillige Zustimmung notwendig sein sollte.

Fraglich könnte nun sein, ob aber der Sender, dass heißt die Bank oder der ISP, auf einer Teilnahme vertraglich bestehen kann. Der ISP etwa würde sich in diesem Fall einen Wettbewerbsvorteil erhoffen, wenn er sich als besonders privatschutzfreundlich differenzieren will. Obgleich, wie Lessig beobachtet hat, Regulierung durch Märkte und Regulierung durch Technologie häufig komplementär sind, ist dieses Modell hier ganz unabhängig von der rechtlichen Frage marktpsychologisch nicht plausibel. Der ISP würde ja etwa so werben müssen: Lieber Kunde, Sie werden wahrscheinlich irgendwann in ihrem Leben von der Polizei verdächtigt werden (unserer Kunden sind so). Da wir uns in solch einem Fall selber nicht trauen würden, aus der polizeilichen Nachfrage so viel über Sie rausfinden zu wollen wie möglich, haben wir ein System eingeführt, dass uns

selber in diesem Fall „blind“ macht. Wir auch Ihr Geld gar nicht wenn Sie an ihm nicht teilnehmen wollen; jeder Kunde ist verpflichtet Mitglied zu werden“. Aus offensichtlichen Gründen werden wenige Unternehmen diese Ansatz wählen. Wahrscheinlicher ist, dass auch sie es Kunden selbst überlassen, ob sie dem Schema beitreten wollen, es aber anbieten, um diejenigen Kunden zu gewinnen, denen ihr Privatschutz besonders wichtig ist. Anders als im Film, in dem jeder Sklave jeden anderen sehen konnte und so „Prisoner dilemma“ Situationen nicht auftreten, stellt sich nun das Problem der „free rider“. Für mich, als Individuum, ist es am besten, nicht selber am Schema teilzunehmen – sofern es genug Freiwillige gibt die es trotzdem am laufen halten. Was passiert in diesem Fall, wenn die Polizei Auskunft über einen Kunden verlangt, der nicht selber dem Schema beigetreten ist? Ist der Sender (Bank, ISP etc) als Verantwortlicher für die Datenverarbeitung berechtigt, hier die weniger sichere Methode der Datenübertragung, also ohne Verschleierer, zu wählen, obgleich es ihm möglich wäre, einen sichereren Weg zu benutzen? Sollte er dazu datenschutzrechtlich gezwungen sein, unterminiert er die Motivation für andere, dem Schema beizutreten, was im Endergebnis zu dessen Zusammenbruch führen kann. Wird dagegen argumentiert, dass der Verdächtige dadurch, dass er nicht beigetreten ist, konkludent eingewilligt hat, dass die weniger sichere Methode verwendet werden darf, so sind wir wieder zurück beim liberalen, individualrechtlichen Begriff der Privatheit. Dieser erlaubt es eben auch, sie gering zu achten und weg zu geben. Dies ist natürlich genau das Verständnis, von dem wir unseren Ansatz in der Einführung abgegrenzt hatten.

Ob letztendlich die gesellschaftlichen Rahmenbedingungen bestehen, um ausreichend Freiwillige zu finden, ist eine empirische Frage, die weiterer Forschung bedarf. Fragen der Loyalität, Gruppensolidarität und gemeinschaftlicher Verantwortung in online Kontexten werden dabei treibende Parameter sein. Für uns war es hier wichtig zu zeigen, dass traditionelle PETs konzeptionell auf einem Verständnis von Privatsphäre und Privatheitsschutz beruhen, dass aber auch anders gedacht werden kann. Ein solches alternatives Verständnis der Privatheit, die sie als kollektives Gut auffasst, erlaubt uns auch die Architektur von PETs neu zu überdenken. Diese sollten aber nicht als Ersatz für andere PETs verstanden werden, sondern nur als ein weiteres Instrumentarium, denn wie unsere abschließende Analyse des gesellschaftlichen und rechtlichen Rahmens gezeigt hat, sind letztendlich kommunitäres und individuell-liberales Privatheitsverständnis aufeinander angewiesen.

Literaturverzeichnis

[Ag03] Agrawal, R., et al: Information sharing across private databases. Paper presented at the Proceedings of the 2003 ACM SIGMOD international conference on Management of data, San Diego, California 2003

[AIR01] Aiello, B., Ishai, Y., & Reingold, O.: Priced Oblivious Transfer: How to Sell Digital Goods. In B. Pfitzmann (Ed.), Advances in Cryptology — EUROCRYPT 2001 (Vol. 2045, pp. 119-135) Berlin: Springer-Verlag 2001

[BD01] Bao, F., & Deng, R.: Privacy Protection for Transactions of Digital Goods. In Information and Communications Security 2001 S 202-213

[Bl64] Bloustein, E J.: , Privacy as an aspect of human dignity: An answer to Dean Prosser, NYUL Rev. 39: 1964 S.962

[Ca99] Cachin, C.: Efficient private bidding and auctions with an oblivious third party. Paper presented at the 6th ACM conference on Computer and communications security - CCS '99, Singapore 1999.

[DA01] Du, W., & Atallah, M. J.: Privacy-Preserving Cooperative Scientific Computations. Paper presented at the Proceedings of the 14th IEEE workshop on Computer Security Foundations 2001

[Fi93] Fine P "Herd immunity: history, theory, practice. Epidemiol Rev 1993 15 (2): S. 265–302.

[Fe6] Ferrari, M. J., Bansal, S., Meyers, L. A., & Bjørnstad, O. N.: Network frailty and the geometry of herd immunity. Proceedings of the Royal Society B: Biological Sciences, 2006 273 S 2743-2748.

[FA03] Frikken, K. B., & Atallah, M. J.: Privacy preserving electronic surveillance. Paper presented at the Proceedings of the 2003 ACM workshop on Privacy in the electronic society, Washington, DC 2003

[GL02] Goldwasser, S., & Lindell, Y. : Secure Computation without Agreement. Paper presented at the Proceedings of the 16th International Conference on Distributed Computing. 2002

[Kw8] Kwecka, Z.et al.: Validation of 1-N OT Algorithms in Privacy-Preserving Investigations. Paper presented at the 7th European Conference on Information Warfare and Security, University of Plymouth 2008.

[KBS10] Kwecka, Z., Buchanan, W. J., & Spiers, D.: Privacy-Preserving Data Acquisition Protocol. Paper presented at the Sibircon, Irkutsk 2010

[OS07] Ostrovsky, R., & William E. Skeith III.: A Survey of Single-Database PIR: Techniques and Applications. In O. Tatsuaki & W. Xiaoyun (Eds.), Public Key Cryptography (Vol. 4450, pp. 393-411). Berlin: Springer 2007

[PH78] Pohlig, S., Hellman, M.: An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (Corresp.), Information Theory, IEEE Transactions 24 1978 S. 106-110

[Ra12] Raab, C.:Privacy, Social Values and the Public Interest, Politische Vierteljahresschrift 46 2012 S.129-152

[Re94] Regan, P. M.: Legislating Privacy: Technology, Social Values and Public Policy, Chapel Hill: The University of North Carolina Press 1994

[Sc95] Schneier, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C: John Wiley & Sons, Inc. 1995

[Sh80] Shamir, A.: On the Power of Commutativity in Cryptography. Paper presented at the Proceedings of the 7th Colloquium on Automata, Languages and Programming 1980

[Sh49] Shannon, C. : Communication theory of secrecy systems. Bell System Technical Journal, 28 1994 S. 656-715

[Sm84] Simitis, S.: Reviewing Privacy in an Information Society, University of Pennsylvania Law Review , 135 1987 S. 707-746

[SS02] Swire, P., & Steinfeld, L.: Security and privacy after September 11: the health care example. Paper presented at the Proceedings of the 12th annual conference on Computers, freedom and privacy, San Francisco, California 2002.

[We06] Weis, S. A.: New Foundations for Efficient Authentication, Commutative Cryptography, and Private Disjointness Testing. Unpublished PhD Thesis, Massachusetts Institute of Technology, Cambridge, MA. 2006

[We84] Weitzman, M.: The share economy: Conquering Stagflation, reprint, Harvard Publication Press, Boston 1984

[Yo06] Young, B. C.,et al: Challenges Associated with Privacy in Health Care Industry: Implementation of HIPAA and the Security Rules. J. Med. Syst., 30(1) 2006 S. 57-64