Rainer Böhme, Andreas Pfitzmann

Digital Rights Management zum Schutz personenbezogener Daten?

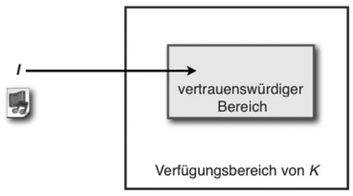
Die Digitalisierung hat bekanntlich die Medienindustrie auf den Kopf gestellt, und es wird immer deutlicher, dass sie Gefahr läuft, bald den Datenschutz ad absurdum zu führen. Was hat dies beides miteinander zu tun? Während Konzepte für nutzerbestimmte datenschutz-fördernde Technik durch Datenvermeidung schon lange etabliert sind, stehen immer wieder Vorschläge zur Realisierung von datenschutzfördernden Systemen durch technisch durchgesetzte Zweckbindung zur Diskussion. Darin soll auf Techniken von Digital Rights Management Systemen zurückgegriffen werden, die von der Medienindustrie zur kontrollierten Verbreitung digitaler Inhalte entwickelt wurden.

1 Von Content-DRM zu Privacy-DRM

Digital Rights Management (DRM) Systeme sind ein Überbegriff für Technologien zur anbieterkontrollierten Nutzung und Verbreitung urheberrechtlich geschützter digitaler Werke. Oft verbindet man sie mit der Vision „sich selbst verteidigender" Mediendaten, welche legitime Nutzer problemlos auf ihren eigenen Geräten konsumieren können, aber beim Versuch illegaler Nutzung unbrauchbar werden. Um dies zu realisieren bestehen DRM-Systeme in der Regel aus einer Reihe von Einzelkomponenten, die verschiedene Schritte in der Verwertungskette von digitalen Inhalten schützen. Je nach Architektur kommen unterschiedliche Technologien zum Einsatz, typischerweise symmetrische oder asymmetrische Verschlüsselung, digitale Signaturen, robuste und fragile digitale Wasserzeichen, Codierungstechniken für Fingerprints, Rechtebeschreibungssprachen (z. B. XrML und ODLR), sowie Trusted-Computing-Techniken basierend auf manipulationssicherer Hardware [PFK02]. Die Analogie zwischen dem bekannten Content-DRM (kurz „C-DRM") zum Schutz von geistigem Eigentum und dem neuen Privacy-DRM (kurz „P-DRM") zum Schutz personenbezogener Daten soll im Folgenden kurz diskutiert werden.

Das „DRM-Problem" für Medieninhalte lässt sich so formulieren: Anbieter *A* will einem Kunden *K* einen Inhalt *I* in einer bestimmten Weise zugänglich machen, ihn aber daran hindern, *alles* damit tun zu können. Die Schwierigkeit besteht darin, dass Inhalt *I* den Vertrauensbereich von *A* verlässt und in den Verfügungsbereich von *K* gelangt, etwa indem die Datei auf dessen eigenen PC abgespeichert wird. Das DRM-Problem kann nur gelöst werden, wenn es *A* gelingt, im Verfügungsbereich von *K* einen Bereich aufzubauen, der für *A* vertrauenswürdig die Inhalte gegen Eingriffe schützt (s. Abb. 1).

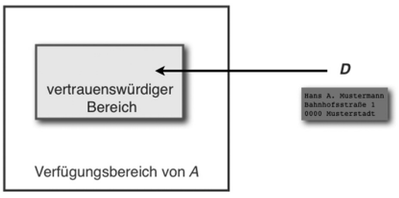
Abbildung 1 | Das „DRM-Problem" für Medieninhalte



Übertragen auf P-DRM folgt: Kunde[1] *K* will einem Anbieter *A* ein personenbezogenes Datum *D* in einer bestimmten Weise zugänglich machen, ihn aber daran hindern, *alles* damit tun zu können. Wiederum bedeutet „zugänglich machen" hier, dass *D* in der EDV von *A* verarbeitet wird, in der nun *K* seinerseits einen vertrauenswürdigen Bereich unterhalten muss (s. Abb. 2).

P-DRM ist für Datenschützer vor allem deshalb interessant, weil es im Gegensatz

Abbildung 2 | Das „DRM-Problem" für Datenschutz



1 Für nicht-kommerzielle Anwendungen könnte Kunde *K* hier durch Bürger *B* ersetzt werden. Wir verzichten auf diese Differenzierung um die Anzahl an Symbolen überschaubar zu halten.

Rainer Böhme

ist wissenschaftlicher Mitarbeiter am Lehrstuhl Datenschutz und Datensicherheit an der Technischen Universität Dresden. Ein Forschungsschwerpunkt sind ökonomische und soziale Aspekte von Datenschutz und Datensicherheit
E-Mail: rainer.boehme@tu-dresden.de

Prof. Dr. Andreas Pfitzmann

Lehrstuhl Datenschutz und Datensicherheit, Institut für Systemarchitektur, Fakultät Informatik, TU Dresden
E-Mail: pfitza@inf.tu-dresden.de

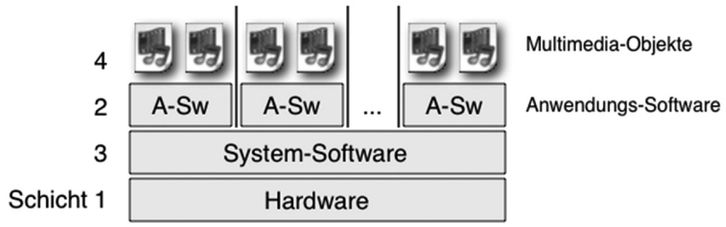
zu anderen Datensicherheitstechniken nicht nur vor unberechtigtem Zugriff durch Dritte schützt, sondern auch die Betreiber von EDV-Systemen als mögliche Angreifer in ihren Handlungsmöglichkeiten beschränkt [Erm07]. Szenarien mit schwächeren Sicherheitsanforderungen sind nicht Gegenstand dieses Aufsatzes.

Im Folgenden wird die Partei an der Datenquelle (*A* bei C-DRM, bzw. *K* bei P-DRM) als *Emittent* bezeichnet. Die Partei, die Inhalte oder Daten in ihren Verfügungsbereich erhält, wird dagegen *Rezipient* genannt. Der Emittent legt Regeln („policies") fest, unter welchen Bedingungen Inhalte *I* bzw. Daten *D* verarbeitet (z. B. abgespielt) werden dürfen, und verknüpft diese als Metadaten mit der Datei (z. B. durch Anhängen oder Einbetten). Typische Regeln für C-DRM können die Wiedergabe des Medieninhalts von einem bestimmten Gerät oder Nutzer abhängig machen bzw. deren Anzahl beschränken. Bei P-DRM könnten die Regeln den Verwendungszweck von personenbezogenen Daten festlegen, den Zugriff nach einer bestimmten Zeit sperren (Löschungsgrundsatz, „digitales Vergessen" [BJ02]), die Weitergabe der Daten regeln, oder möglicherweise bestimmte Data-Mining-Technologien verbieten bzw. für hinreichend anonymisierte Statistiken auch explizit erlauben.

Für die Überprüfung und Durchsetzung der Regeln ist im Einzelfall die Implementierung des vertrauenswürdigen Bereichs auf dem System des Rezipienten verantwortlich. Besonders komplizierte Regeln oder solche, die von externen und auf dem System des Rezipienten nicht verlässlich rekonstruierbaren Bedingungen abhängen, können auch „online" entschieden werden. Dazu ist ein Kommunikationskanal erforderlich, über den vor jeder Verarbeitung eine Erlaubnisanfrage an einen Server des Emittenten gestellt werden kann. Es ist offensichtlich, dass auch die Integrität der Regeln sowie ggf. der Kommunikation mit dem Server sichergestellt sein muss, sonst ließe sich über eine geeignete Manipulation die Wirksamkeit des DRM-Systems leicht aushebeln.

Abbildung 3 zeigt die Ausführungs-Schichtenstruktur von gängigen Multimedia-PCs. Weil Objekte vor den darunter liegenden Schichten nicht effektiv geschützt werden können, ist es auf frei programmierbaren PCs unmöglich, sichere geschützte Bereiche für Inhalte *I* oder personenbezogene Daten *D* herzustellen. Viele praktische DRM-Systeme belassen es daher bei einem unvollkommenen und, da auf Geheimhaltung von Dokumentation beruhendem („security by obscurity"), zeitlich begrenzten Schutz.

Abbildung 3 | Ausführungs-Schichtenstruktur: Objekte können vor darunter liegenden Schichten nicht effektiv geschützt werden.



2 Lehren aus Erfahrung mit Content-DRM

Seit etwa zehn Jahren wird immer wieder versucht, DRM-Systeme zum Schutz von Medieninhalten in der Praxis einzusetzen. Sichere Systeme können dabei im Wesentlichen nach zwei verschiedenen Architekturen konzipiert werden, die hier kurz in Form von idealtypischen Ansätzen vorgestellt werden.[2]

Die Vision früher DRM-Entwickler lag in einer *offenen Architektur mit Rückverfolgungsmöglichkeit*. Kern dieser Architektur ist das Einbetten von kundenspezifischen Kennzeichen in die Mediendaten mit Hilfe von *robusten digitalen Wasserzeichen* [Ditt00]. Digitale Wasserzeichen werden eingebracht, indem man Medieninhalte an für den Menschen nicht wahrnehmbaren Stellen so verändert, dass ein so genannter *Wasserzeichen-Detektor* mit Kenntnis eines entsprechenden Schlüssels ein zuvor definiertes Kennzeichen mit hinreichender Sicherheit nachweisen kann.

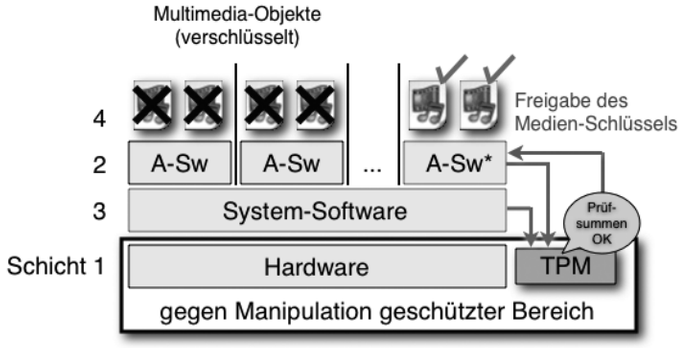
Nach gängigen Sicherheitsdefinitionen soll es dabei einem Kunden ohne Kenntnis des Schlüssels nicht gelingen, das Wasserzeichen aus den Mediendaten zu entfernen bzw. unlesbar zu machen, ohne dabei gleichzeitig die Qualität des Mediums auf ein nicht mehr schützenswertes Niveau zu reduzieren. Ein robustes digitales Wasserzeichen mit kundenspezifischen Kennzeichen wird als *Fingerprint* bezeichnet. Sichere Fingerprints sind mindestens so schwierig zu realisieren wie sichere robuste digitale Wasserzeichen: Erstens muss ausgeschlossen werden, dass der Fingerprint mit einem Angriff auf das Wasserzeichenverfahren unkenntlich gemacht werden kann. Zweitens könnten Manipulationen am Fingerprint zur Verdächtigung unschuldiger Kunden führen, indem der Angreifer den Wert des Kennzeichens verändert, ohne den Fingerprint dabei unkenntlich zu machen. Und drittens muss das Angreifermodell berücksichtigen, dass Kunden in einer Koalition zusammenarbeiten können und so die Differenzen ihrer Mediendaten zum Lokalisieren und Entfernen des Fingerprints benutzen.

Bei der offenen DRM-Architektur wird die Wirksamkeit des Schutzes gegen illegale Nutzung (insbesondere unkontrollierte Weiterverbreitung) allein durch das Drohpotenzial erreicht, Kunden für illegale Kopien, die mit ihrem Kundenkennzeichen versehen sind, haftbar zu machen. Damit soll sicher gestellt werden, dass Kunden im eigenen Interesse mit den Medieninhalten verantwortlich umgehen. Robuste digitale Wasserzeichen sind – wie dargelegt – unbedingt notwendig, um eine irreversible Verkopplung der Kundenkennzeichen mit den Medieninhalten zu erreichen.

Bei der *geschlossenen Architektur* werden dagegen Sicherheitseigenschaften durch Eingriffe in die Ausführungs-Schichtenstruktur realisiert. Dies kann durch dezidierte Wiedergabehardware geschehen, die nicht frei programmierbar ist und – sofern sie Geheimnisse der Inhalteanbieter enthält – gegen Manipulationen und *reverse engineering* physisch geschützt ist (Beispiel: DVD-Player, Pay-TV-Decoder). Mediendaten können dabei in verschlüsselter Form über nicht vertrauens-

2 Es sind noch weitere Ansätze denkbar, die allerdings auf zu optimistischen Annahmen basieren (kein Reverse-Engineering von Software) und damit schon theoretisch keinen wirksamen Schutz gegen starke Angreifer erreichen können. Das heißt jedoch nicht, dass diese Ansätze im Zeitverlauf nicht versucht wurden. Für Datenschutzzwecke sind sie aber nicht zu empfehlen.

Abbildung 4 | Die Rolle von TPM in der Ausführungs-Schichtenstruktur



würdige Netze und PCs von Kunden übertragen werden.

Eine Entschlüsselung und Wiedergabe erfolgt dabei erst in der Hardware, die einen Vertrauensbereich des Anbieters darstellt. Mit Techniken des so genannten *trusted computing* kann auch auf frei programmierbarer Hardware, die allerdings gegen physische Manipulationen des Besitzers geschützt sein sollte, ein solcher Vertrauensbereich hergestellt werden.

Die wohl bekannteste Lösung funktioniert mit einem so genannten *Trusted Platform Module* (TPM), das die Funktionalität besitzt, Geheimnisse – auch vor dem Besitzer der Hardware – sicher zu verwahren und Prüfsummen über Programme im Arbeitsspeicher eines PCs zu verwalten.[3] Nur wenn diese Prüfsummen mit vom Anbieter definierten zulässigen Referenzwerten übereinstimmen, wird das TPM die Entschlüsselung von Mediendaten freigeben (i.d.R. durch Einsatz seiner Geheimnisse, sonst könnte die Freigabe auch durch Dritte erreicht werden). Die eigentliche Entschlüsselung kann dann in Software erfolgen, da Anbieter nur Prüfsummen von solchen Programmen zulassen, denen sie vertrauen, dass die Datenverarbeitung nicht gegen ihre Interessen geschieht (Abb. 4).

Geschlossene DRM-Architekturen kommen ohne Wasserzeichen aus, verlassen sich aber auf die Manipulationssicherheit von Hardware (im Beispiel: TPM *und* programmausführende Hardware) und oft auch auf die Fehlerfreiheit von Software.

Keine der beiden Architekturen hat sich bisher in der Praxis in reiner Form bewährt, so dass alle kommerziell eingesetzten C-DRM-Systeme Elemente aus beiden Ansätzen vereinen [Katz04].

- Probleme der geschlossenen Architektur sind hohe Kosten von ausreichend sicherer Spezialhardware, die bisher zögerliche Verbreitung von TPMs, sowie das so genannte „*analog hole*". Damit ist die Möglichkeit gemeint, dass Kunden die Wiedergabe eines Medieninhalts „anstelle eines Sinnesorgans" aufzeichnen, etwa durch Abfilmen eines Monitors, und ggf. danach erneut digitalisieren.
- Schwächen der offenen Architektur liegen vor allem daran, dass Technologien für wirklich sichere robuste digitale Wasserzeichen nicht einmal ansatzweise zur Verfügung stehen. Zum wiederholten Male wurden als sicher geltende Wasserzeichen-Verfahren in Wettbewerben zum Brechen freigegeben und es ist kein Fall bekannt, in dem selbst die unter Laborbedingungen erstellten Wasserzeichen den Angriffen standgehalten haben.

Dies ist umso beachtlicher, wenn man bedenkt, dass diese Wettbewerbe unter (für den Angreifer) unrealistisch erschwerten Bedingungen durchgeführt werden: Bei der SDMI-Challenge wurden weniger Informationen veröffentlicht, als ein realer Angreifer beim Einsatz des DRM-Systems zur Verfügung hätte. Die aktuelleren BOWS-Contests[4] schränken Angreifer durch die Wahl eines unrealistischen Qualitätsmaßes derart ein, dass ganze Klassen von besonders wirkungsvollen geometrischen Angriffen [PAK98] nicht verwendet werden können.

Weitere Probleme beim Einsatz von Fingerprints sind die bei vielen Implementierungen mangelnde Beweiskraft von Nachweisen des Kunden- [PS96] oder Anbieterkennzeichens [CM+98] sowie Akzeptanzprobleme, wenn der Verlust eines portablen Abspielgeräts mit einer möglichen Schadenersatzforderung durch Weiterverbreitung der mit dem eigenen Kennzeichen versehenen Medieninhalte einhergeht. Ergänzender Schutz wird durch den Einsatz weiterer Mechanismen erreicht:

- Hersteller von Konsumelektronik statten ihre Geräte (Videokameras, Scanner) mit Wasserzeichen-Detektoren aus und programmieren die Geräte so, dass sie die Aufzeichnung oder Verarbeitung von als geschützt markierten Mediendaten verweigern. Ein derartiger Schutz erschwert beispielsweise die Digitalisierung von Banknoten [Mur04].
- Weiterhin suchen Inhalteanbieter selbst nach illegalen Kopien ihrer Medieninhalte im Internet und in Filesharing-Communities und versuchen durch *technische Zugriffsfilter* und *Sperren* eine Verbreitung zu unterbinden [PFK02].
- Beim DVD-Standard wurde versucht, durch Einführung von *Regional-Codes* und je nach Kontinent unterschiedlicher Wiedergabehardware die weltweite Verbreitung von Inhalten zu behindern.
- Nicht zuletzt sind mit dem *Digital Millennium Copyright Act* (DMCA) und den daran angelehnten Gesetzen rechtliche Rahmenbedingungen geschaffen worden, die Anbietern eine Verfolgung von Missbrauchsfällen erleichtern sowie die Entwicklung und Verbreitung von Werkzeugen zur Umgehung der technischen Schutzmaßnahmen unter Strafe stellen.[5]

Trotzdem ist DRM für Medieninhalte keine Erfolgsgeschichte. Praktisch jeder Schutz wurde geknackt und die „befreiten" Medieninhalte sind nach dem BORE-Prinzip („*break once, run everywhere*" [And03]) für versierte und geduldige Nutzer mit Breitbandanschluss im Internet frei erhältlich. Kunden klagen über Inkompatibilitäten und sehen sich als Opfer von Sicherheitsproblemen (Stichwort Sony-Rootkit [HF06]). Ökonomen kritisieren den gesellschaftlichen Schaden durch

3 Siehe Schwerpunkthefte DuD 9/2004 und 9/2005.

4 Siehe http://lci.det.unifi.it/BOWS/ (2006) bzw. http://bows2.gipsa-lab.inpg.fr/ (2007)

5 Mit Hilfe dieses Gesetzes wurde leider auch versucht, kritische Stimmen aus der Wissenschaft zu bestimmten DRM-Technologien mundtot zu machen [Cr+01]. Außerdem ist die rechtliche Abgrenzung von Umgehungswerkzeugen höchst problematisch.

Inkompatibilitäten zwischen konkurrierenden DRM-Systemen, die zu Wettbewerbsverzerrungen führen und Konsumenten in einer Plattform „einsperren" (*lock-in*) [Eco06].

Folglich findet bei der digitalen Distribution von Musik bereits ein Umdenken statt. Marktführer Apple bietet seit Mitte 2007 DRM-freie Stücke zum Download über die iTunes-Plattform an. Die Filmindustrie hat aber anscheinend die Hoffnung noch nicht ganz aufgegeben [JL07].

3 Von der Analogie zum Antagonismus

Die Verwendung von DRM-Techniken für den Datenschutz hört sich bei oberflächlicher Betrachtung viel versprechend an; die Gemeinsamkeiten erscheinen absolut einleuchtend. Der zweite, genauere Blick offenbart allerdings Unterschiede zwischen den Anwendungsfällen, die technisch und organisatorisch anderer Lösungen bedürfen. Zur Diskussion der Unterschiede zwischen C-DRM und P-DRM betrachten wir zunächst die zu schützenden Daten, dann Aspekte der Organisation und Kontrolle sowie schließlich die Größenordnung der notwendigen Entwicklungskosten.

3.1 Unterschiede in den Eigenschaften der zu schützenden Daten

Digitale Medieninhalte und digitale Repräsentationen von personenbezogenen Daten unterscheiden sich mindestens in drei wesentlichen Punkten:

1. dem Anteil an Irrelevanz,
2. der Wertentwicklung im Zeitverlauf, und
3. der Sensibilität pro Bit.

Zu 1. (Anteil an Irrelevanz)

Multimediadaten enthalten – trotz verlustbehafteter Kompression, da diese nie perfekt ist – einen großen Anteil an Irrelevanz, die sich nicht eindeutig von der Information trennen lässt[6] (sonst könnte man durch eine Trennung die verlustbehaftete Kompression verbessern). Digitale Wasserzeichen, als notwendige Bestandteile von DRM-Systemen der offenen Architektur, betten verschlüsselte Informationen in die Bereiche der Mediendaten ein, die mit sehr hoher Wahrscheinlichkeit irrelevant sind. Robuste Wasserzeichen werden mit Hilfe von Fehlerkorrekturcodes redundant eingebettet, so dass auch für kurze verschlüsselte Informationen (wie z.B. ein Kundenkennzeichen) relativ viele Stellen am Medium geändert werden müssen. Personenbezogene Daten (Adresse, Bankverbindung, Familienstand etc.) sind dagegen sehr diskret, so dass die Einbettung von robusten digitalen Wasserzeichen ohne Änderung der Semantik praktisch unmöglich ist.

Dies kann übrigens auch nicht durch künstliches Hinzufügen von Irrelevanz vor der Einbettung kompensiert werden, da personenbezogene Daten oft in eine kanonische Form gebracht werden können, womit die Information vom Wasserzeichen trennbar wäre. Als Beispiel sei die Technik mit erfundenen Initialen zum Adress-Fingerprinting genannt. Um zu erforschen, wer personenbezogene Daten von Hans Mustermann verkauft, könnte er ein bisschen flunkern und Anbieterkennzeichen in seine Anschrift einfügen: Hans *A.* Mustermann für *Amazon.com*, Hans *B.* Mustermann für seine *Bank*, usw. Ein Abgleich mit einem Adressverzeichnis würde jedoch den zusätzlichen Initial verschwinden lassen und so den „Fingerprint" entfernen. Da digitale Wasserzeichen zum Schutz der eigenen personenbezogenen Daten im Allgemeinfall[7] nicht zur Verfügung stehen, müsste also ein P-DRM-System grundsätzlich in einer geschlossenen Architektur aufgebaut sein.

Zu 2. (Wertentwicklung im Zeitverlauf)

Mit fortschreitender Zeit verlieren Medieninhalte tendenziell ihren kommerziellen Wert. Immer mehr Menschen haben einen Film schon gesehen, die Mode und der Geschmack ändern sich, Filme und Musik wurden im Fernsehen bzw. auf Sammel-CDs sekundär verwertet. Manche C-DRM-Mechanismen sind vor dem Hintergrund dieses Wertverlustes konzipiert. So können Schlüssel für kompromittierte Hersteller bzw. bei neueren Standards einzelne Wiedergabegeräte nur auf neu aufgelegten Medien zurückgezogen werden [JL07]. Bis auf wenige Ausnahmen (Entscheidung über Nutzungsgewährung erfolgt online) werden Sperren also nur für neue Medieninhalte wirksam. Bei personenbezogenen Daten können keine eindeutigen Aussagen zur Entwicklung der Sensibilität im Zeitverlauf gemacht werden. Berücksichtigt man allerdings, dass Menschen ihr Wesen in der Regel nur langsam ändern, so könnte es vielen Menschen schwer fallen, mit sehr weit zurück liegenden personenbezogenen Daten („Dummheiten aus der Abizeit") umzugehen.

Auch die Theorie, digitale Daten automatisch zu „vergessen" sei gesellschaftlich wünschenswert und würde den sozialen Realitäten vor der Digitalisierung näher kommen, unterstellt implizit, dass ältere personenbezogene Daten in den falschen Händen schädlicher sind als jüngere [BJ02]. Wir können also nicht davon ausgehen, dass personenbezogene Daten ähnlich wie Medieninhalte mit der Zeit wertloser werden. DRM-Technologien, die auf dieser Prämisse aufbauen, sind damit für P-DRM ungeeignet.

Zu 3. (Sensibilität pro Bit)

Personenbezogene Daten sind, bezogen auf ihr Volumen, wesentlich sensibler als Multimediadaten. Der monetäre Verlust von zwei illegalen Kopien von Musik-CDs liegt, unter Annahme des vollen Brutto-Ladenpreises, bei ca. 32 Euro. Sollten diese von 10 weiteren Personen kopiert werden, die sonst die CDs gekauft hätten (!), summiert sich der Schaden auf 320 Euro. Ende November 2007 wird bekannt, dass den britischen Finanzbehörden zwei CDs mit personenbezogenen Daten (u.a. Bankverbindung aller britischen Kindergeldempfänger) abhanden gekommen sind – zusammen 25 Millionen Datensätze.[8] Nach Schätzungen der Firma Trend-

6 Die Begriffe Information, Redundanz und Irrelevanz werden nur in diesem Absatz in einem informationstheoretisch engen Sinn verwendet [KPS06].

7 Der Vollständigkeit halber seien hier zwei Ausnahmen genannt. Erstens: Mit zunehmendem Gebrauch von *biometrischen Merkmalen* könnten in Zukunft Klassen von personenbezogenen Daten verarbeitet werden, die einen höheren Anteil Irrelevanz enthalten. Zweitens: Fingerprinting von *Sammlungen* personenbezogener Daten kann durchaus funktionieren. Hier kann Information in der Tatsache versteckt werden, ob eine – tatsächlich existierende – Adresse in kanonischer Form Bestandteil der Sammlung ist oder nicht. So werden bspw. gegenwärtig Adresslisten mit Empfängeradressen für Direktmarketing-Sendungen vor mehrmaliger Verwendung geschützt: Der Mieter einer Adressliste weiß nicht, welcher Empfänger dem Vermieter als Kontrolladresse dient.

8 Siehe http://www.lightbluetouchpaper.org/2007/11/20/government-security-failure/ (November 2007)

Micro[9] lag der Schwarzmarktpreis für eine gültige Kombination aus Anschrift, Bankverbindung und Geburtsdatum zwischen 80 und 300 USD. Selbst eine vorsichtige Hochrechnung unter der Annahme, dass nur jede zehnte Adresse 80 USD wert ist, ergibt die horrende Summe von knapp 140 Mio. Euro. Der um Größenordnungen höhere Wert von personenbezogenen Daten macht sie zum Ziel von mächtigeren Angriffen und erfordert entsprechend hohe Standards bei der Sicherheitstechnik.

3.2 Unterschiede der Organisation und Kontrolle

Bei einer geschlossenen DRM-Architektur muss der Emittent den geschützten Bereich auf dem System des Rezipienten kontrollieren. Wäre die Realität wie unsere bisherige Betrachtung auf nur zwei Parteien beschränkt, so gäbe es kaum Unterschiede zwischen C-DRM und P-DRM. In der Realität haben wir es bei C-DRM jedoch mit wenigen Anbietern zu tun, die jeweils die Endgeräte vieler Kunden kontrollieren. Würde die gegenwärtige Praxis der Inkompatibilität zwischen DRM-Systemen unterschiedlicher Anbieter beibehalten, dann würde jedes Endgerät von genau einem Anbieter kontrolliert. Alternativ könnten die Anbieter zusammen mit Hardware- und Betriebssystemherstellern eine Verwertungskoalition bilden, die sich gegenseitig vertraut und ihre gleichgerichteten Interessen durchsetzt.

Übertragen auf P-DRM wäre der erste Fall (Inkompatibilität) überhaupt nicht vorstellbar. Im zweiten Fall (Koalition) müssten sich Millionen Kunden – mit heterogenen Interessen – zusammenschließen und die EDV von vielen Anbietern kontrollieren. Auch dies scheint eher unrealistisch (wie auch in ähnlich lautenden Vorschlägen [ZD04] und [SSA06]). Vielmehr müsste man überlegen, ob die Kunden bei P-DRM die Kontrolle an eine vertrauenswürdige Datenschutz-Autorität delegieren können. Diese Instanz müsste dann die EDV aller mit personenbezogenen Daten operierenden Organisationen regelmäßig (und unangekündigt) überprüfen können. Gleichzeitig müsste sichergestellt werden, dass die Instanz in der Wahrnehmung ihrer kritischen Aufgabe nicht unkontrollierbar mächtig wird.

Dieser Machtkonzentration auf Kontrollebene könnte nur mit einer Verteilung der Kontrollaufgaben auf mehrere unabhängige Kontrollbehörden begegnet werden. Allerdings ist unklar, ob dies ohne Effektivitätsverluste realisierbar ist (von Effizienz ganz zu schweigen).

Auch die im C-DRM ergänzend eingesetzten technischen Zugriffsfilter und Sperren sind für P-DRM nur bedingt geeignet. Weder einzelne Nutzer noch eine Kontrollinstanz werden in der Lage sein, aktiv in Business-to-Business (B2B)-Netzwerken nach illegal ausgetauschten Kundendaten zu suchen und diesen Austausch technisch zu blockieren. Allein die Verwendung von Regional-Codes für P-DRM erscheint umsetzbar, wenn auch – wie bei der DVD – nur begrenzt wirksam. Damit könnte zumindest technisch sichergestellt werden, dass ehrliche Datenverarbeiter nicht aus Versehen personenbezogene Daten in andere Jurisdiktionen übertragen, wo die mit dem Kunden vereinbarten Datenschutzgrundsätze unter Umständen nicht gelten.

Schließlich ist ein nach dem Vorbild des DMCA entworfenes Gesetz zum Verbot der Entwicklung und des Besitzes von Data-Mining-Software vermutlich genauso wenig hilfreich wie der DMCA und der so genannte „Hacker-Paragraf" § 202c StGB.

3.3 Unterschiede in der Höhe der Entwicklungskosten

Zu guter Letzt ein ökonomisches Kalkül: Ein C-DRM System ist kommerziell erfolgreich, wenn es den Missbrauch von Medieninhalten spürbar reduziert (90% wäre ein großer Erfolg). Was die anderen 10% der Nutzer mit den Inhalten tun, ist den Rechteinhabern weitestgehend egal (solange sie keine Super-Distribution initiieren). Übertragen wir das auf Datenschutz: Ein P-DRM-System, das 90% der Institutionen und Privatpersonen dazu bringt, sich an die vereinbarten Regeln zu halten, mag zwar bereits ein Fortschritt gegenüber heute sein. Ob wir dies als großen Erfolg bezeichnen sollten, ist jedoch fraglich.

Kurzum: Soll DRM für Datenschutz einen wesentlichen Beitrag leisten, muss DRM nahezu perfekt funktionieren. Für einen wesentlichen Beitrag zum Schutz von geistigem Eigentum reicht weniger Sicherheit. Die Kosten eines Systems steigen mit dem Grad an erzielter Sicherheit und zwar mit abnehmendem Grenznutzen: Jede zusätzliche Investition in Sicherheit wird teurer, je höher das Sicherheitsniveau bereits ist[10] [GL02].

Deshalb wird die Medienindustrie keinesfalls die Entwicklung von DRM-Werkzeugen bis zu einem solchen Grad an Wirksamkeit finanzieren, dass sie für Datenschutz wirklich interessant werden. Dabei bleibt fraglich, ob sich die Sicherheit von DRM-Systemen überhaupt genügend steigern lässt – selbst wenn man bereit wäre, horrende Kosten in Kauf zu nehmen.

4 Fazit

Die Gemeinsamkeiten zwischen Datenschutz und dem Schutz geistigen Eigentums erscheinen zunächst verblüffend und folglich eine Übertragung der Technologien viel versprechend. Eine genauere Analyse der Voraussetzungen und Anforderungen in diesem Aufsatz hat jedoch ergeben, dass (1) selbst DRM für Medieninhalte heute sehr fehleranfällig ist und (2) Privacy-DRM unter technisch deutlich ungünstigeren Voraussetzungen noch höhere Anforderungen erfüllen müsste. Digitale Wasserzeichen, eine Kerntechnologie heutiger Medieninhalte-DRM-Technik, können für Privacy-DRM praktisch nicht eingesetzt werden.

Privacy-DRM müsste also grundsätzlich anders realisiert werden, nämlich unter Einsatz von manipulationssicherer vertrauenswürdiger Hardware. Selbst dann ist keine Technik bekannt, um das Problem des *analog hole* beim Datenschutz zu lindern. Da Adresshändler heute bereits Klingelschilder abschreiben sowie Kleinanzeigen und Telefonbücher eintippen lassen, werden sie keinen Aufwand scheuen, um personenbezogene Daten von der Ausgabe DRM-geschützter Systeme in eigene,

9 Siehe http://www.informationweek.com/blog/main/archives/2007/02/a_walk_through.html (Februar 2007)

10 Diese Annahme lässt sich theoretisch auf mindestens zwei Arten rechtfertigen. Erstens, ausgehend von einem völlig ungesicherten System sind die möglichen Sicherheitsmaßnahmen unterschiedlich teuer. Ein rationaler Investor würde zunächst die günstigen Maßnahmen ergreifen, so dass später nur noch die teuren übrig bleiben. Zweitens sind Sicherheitsmaßnahmen in der Regel nicht unabhängig voneinander. Die Anzahl der zu berücksichtigenden Interdependenzen wächst mit der Zahl der Maßnahmen.

nicht DRM-geschützte EDV einzugeben.[11]

Umgekehrt gilt: Sollte Privacy-DRM jemals sicher funktionieren, dann steht auch einer lückenlosen Kontrolle der Medieninhalte technisch wohl nichts mehr im Wege.

Danksagung

Für konstruktive Hinweise und Diskussionen bedanken wir uns bei Mike Bergmann, Stefan Berthold, Marit Hansen, Matthias Kirchner, Stefan Köpsell, Jan Schallaböck und Dr. Dagmar Schönfeld.

Literatur

[And03] Anderson, R. (2003): Trusted Computing FAQ 1.1 – deutsch. Online unter http://moon.hipjoint.de/tcpa-palladium-faq-de.html (letzter Abruf: Nov 2007)

[BJ02] Blanchette, J.-F. und Johnson, D. G. (2002): Data retention and the panoptic society: The social benefits of forgetfulness. *Information Society* 18 (1), S. 33-45

[Cr+01] Craver, S. et al. (2001): Reading between the lines: Lessons from the SDMI challenge. *Proc. of the 10th USENIX Security Symposium*, USENIX Association, Washington, DC. Online unter http://www.usenix.org/events/sec01/craver.pdf (letzter Abruf: Nov 2007)

[CM+98] Craver, S., Memon, N., Yeo, B. L. und Yeung, M. M. (1998): Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications. *IEEE Journal on Selected Areas in Communications* 16 (4), S. 573-586

[Ditt00] Dittmann, J. (2000): Digitale Wasserzeichen: Grundlagen, Verfahren, Anwendungsgebiete. Springer Verlag, Berlin

[Eco06] o.V. (2006): Apples are not the only fruit (Economics focus). *The Economist* 380, 6. Juli 2006

[Erm07] Ermert, M. (2007): Persönliches DRM als Retter von Datenschutz und Privatsphäre. *Heise Online*, 18. November 2007. Online unter http://www.heise.de/newsticker/meldung/99163 (letzter Abruf: Jan 2008)

[GL02] Gordon, L. A. und Loeb, M. P. (2002): The economics of information security investment. *ACM Trans. on Information and System Security* 5 (4), S. 438-457

[HF06] Halderman, A. und Felten, E. (2006): Lessons from the Sony CD DRM episode. *Proc. of the 15th USENIX Security Symposium*, USENIX Association, Berkeley, CA.

[JL07] Jin, H. und Lotspeich, J. (2007): Renewable traitor tracing: A trace-revoke-trace system for anonymous attack. In J. Biskup und J. Lopez (Hrsg.): *Computer Security – ESORICS 2007*. Band 4734 der Reihe LNCS. Springer Verlag, Berlin, S. 563-577

[Katz04] Katzenbeisser, S. (2004): On the integration of watermarks and cryptography. In T. Kalker et al. (Hrsg.): *Proc. of International Workshop on Digital Watermarking*. Band 2939 der Reihe LNCS. Springer Verlag, Berlin, S. 50-60

[KPS06] Klimant, H., Piotraschke, R. und Schönfeld, D. (2006): *Informations- und Kodierungstheorie*. 3. Auflage, Teubner Verlag, Wiesbaden

[Mur04] Murdoch, S. (2004): *Software Detection of Currency*. Online unter http://www.cl.cam.ac.uk/~sjm217/projects/currency/ (letzter Abruf: Nov 2007)

[PAK98] Petitcolas, F., Anderson, R. und Kuhn, M. (1998): Attacks on copyright marking systems. In D. Aucsmith (Hrsg.): *Information Hiding, Second International Workshop*. Band 1525 der Reihe LNCS. Springer Verlag, Berlin, S. 219-239

[PFK02] Pfitzmann, A., Federrath, H. und Kuhn, M. (2002): Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität technischer Schutzmechanismen. Studie im Auftrag von dmmv und VPRT. Online unter http://www.cl.cam.ac.uk/~mgk25/dmmv-gutachten.pdf (letzter Abruf: Nov 2007)

[PS96] Pfitzmann, B. und Schunter, M. (1996): Asymmetric fingerprinting. In U. Maurer (Hrsg.): *Advances in Cryptology – EUROCRYPT*. Band 1070 der Reihe LNCS. Springer Verlag, Berlin, S. 84-95

[SSA06] Sackmann, S., Strücker, J. und Accorsi, R. (2006): Personalization in privacy-aware highly dynamic systems. *Communications of the ACM* 49 (9), S. 32–38

[ZD04] Zwick, D. und Dholakia, N. (2004): Whose identity is it anyway? Consumer representation in the age of database marketing. *Journal of Macromarketing* 24 (1), S. 31-43

11 Einschränkend ist anzumerken, dass das *analog hole* nur dann existiert, wenn personenbezogene Daten im Verarbeitungsprozess ausgegeben und somit „rezipiert" werden (können). Es sind durchaus spezielle Verwendungszwecke denkbar, die keiner Art von Ausgabe oder manueller Kontrolle bedürfen. Mögliche Beispiele sind die Erstellung von aggregierten Statistiken (z.B. Zensus) oder die Datenhinterlegung für Notfälle (deren Eintritt wohl definiert und verifizierbar ist).