Institut für Internet-Sicherheit – if(is)

# Online Privacy Service

Ein zukunftsweisender Lösungsvorschlag für eine aktive informationelle Selbstbestimmung im Internet

Maik Heidisch, Prof. Norbert Pohlmann
16.11.2012

# Inhaltsverzeichnis

# Ausgangslage des Datenbriefs

## Datenschutz im Internet

Die Betreiber von Social Networks, wie beispielsweise Facebook und Google+ verdienen ihr Geld vor allem mit Werbung. Die Nutzer dieser Netzwerke zahlen zunächst nichts für den jeweiligen Internet-Dienst, geben jedoch im Gegenzug unzählige persönliche Daten über sich preis. Die Erhebung, Speicherung und Weiterverarbeitung dieser Nutzerdaten sichern die Betreiber mithilfe ihrer AGB. Diesen müssen die Nutzer während der Anmeldung zustimmen. Aus den erhobenen persönlichen Daten der Nutzer erstellen Betreiber sozialer Netze Nutzerprofile, die für den Verkauf von Waren und Dienstleistungen genutzt werden, weil sie passgenaue, individualisierte Werbung ermöglichen. Zielgenaue Werbung lassen sich die Betreiber vieler sozialer Netzwerke durch das Schalten von individualisierten Anzeigen gut bezahlen. Dieses Prinzip „Bezahlen mit persönlichen Daten“ wird auch bei anderen Diensten wie Suchmaschinen, E-Mail-Diensten und Nachrichten-Diensten. angewendet. Aber auch im Bereich von E-Commerce wie beispielsweise. Amazon werden persönlichen Daten erhoben, gespeichert und ausgewertet, um den Kunden individuelle Angebote machen zu können.

In Deutschland gibt es das Recht auf informationelle Selbstbestimmung. Dieses Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Bislang sind Nutzer allerdings überhaupt nicht bzw. kaum Herr ihrer persönlichen Daten im Internet.

## Der Datenbrief als Forderung des Chaos Computer Clubs

Als Forderung des Chaos Computer Clubs sollen Firmen, Behörden und Institutionen, die personenbezogene Daten erheben, verpflichtet werden, in regelmäßigen Abständen kostenlose Information über die gespeicherten Daten an die Betroffenen zu versenden. Dies beinhaltet auch „angereicherte Daten“, wie zum Beispiel Profile und Scoring-Werte. Ein Datenbrief würde die informationelle Selbstbestimmung maßgeblich stärken. Im Moment hat ein Betroffener nach dem Bundesdatenschutzgesetz ein Recht auf Auskunft (vgl. §§ 19, 34 BDSG). Es muss jedoch dazu bekannt sein, an welchen Stellen Informationen über den Betroffenen gespeichert sind. Anschließend muss der Bürger als Bittsteller gegenüber der speichernden Stelle auftreten. Dies wird oft durch eine aufwendige Identifikation mittels einer Kopie des Personalausweises oder des PostIdent-Verfahrens erschwert.

# Konzept

## Die Idee des Online Privacy Service

Mit dem Online Privacy Service (oder auch „Elektronischen Datenbrief“) stellt das Institut für Internet-Sicherheit einen zukunftsweisenden Lösungsvorschlag für die Anbieter von Internet-Diensten vor, wie eine aktive informationelle Selbstbestimmung im Internet umgesetzt werden kann. Der Großteil der Kritik am Konzept des Datenbriefes konzentriert sich auf die Art der Zustellung, speziell auf das Problem der Fehladressierung und dem damit verbundenen Missbrauchspotential. Der Online Privacy Service verpflichtet daher Firmen, Behörden und Institutionen, die personenbezogene Daten erheben und Anbieter eines Internet-Dienstes sind, den Betroffenen die Informationen über die gespeicherten Daten regelmäßig kostenlos über einen standardisierten Elektronischen-Datenbrief-Dienst (Online Privacy Service) zur Verfügung zu stellen. Dieser Online Privacy Service oder Elektronische-Datenbrief-Dienst muss in den bestehenden Internet-Dienst integriert sein, damit der Zugriff mit den gleichen Zugangsdaten möglich ist. Jeder Internet-Dienst muss analog zum Datenbrief alle über den Betroffenen gespeicherten Daten sowie deren Ursprung enthalten und auch zeigen, ob und wenn ja, welche Daten an eine dritte Stelle übermittelt wurden. Zudem muss der Zweck und Rechtsgrundlage für die Speicherung und Übermittlung und eine Widerspruchs- und Korrekturmöglichkeit enthalten sein. Die Widerspruchs- und Korrekturmöglichkeit impliziert ebenfalls, auch alle nicht für den ordnungsgemäßen Betrieb des Internet-Dienstes erforderlichen Daten, wie zum Beispiel für Werbezwecke angereicherten Daten, komplett löschen zu können.

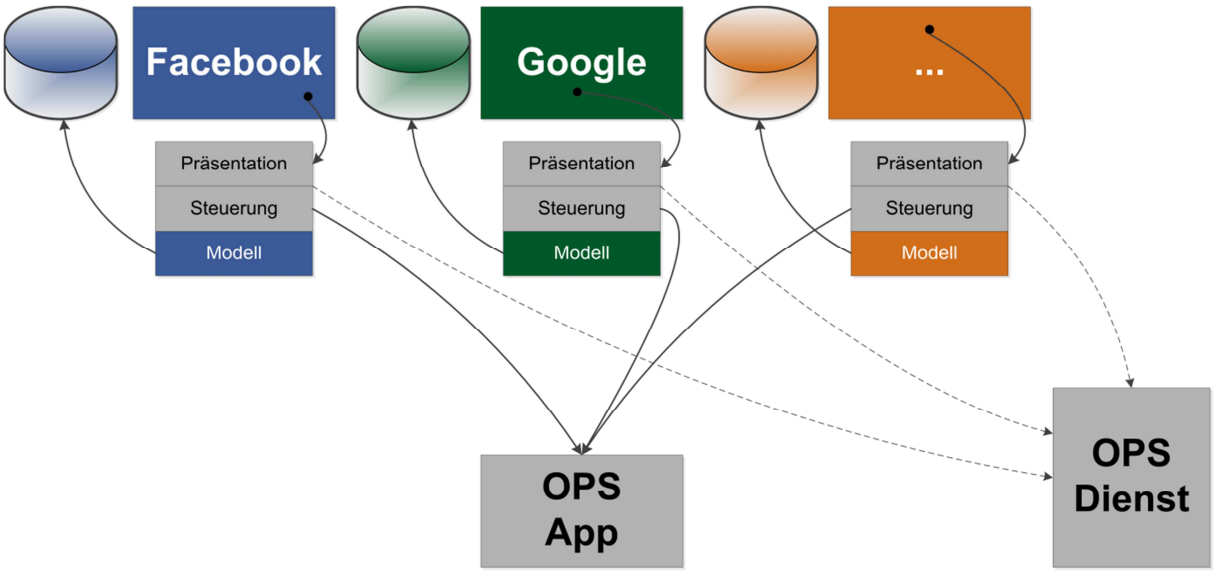
## Lösung der Probleme des ursprünglichen Datenbriefkonzepts

Der Online Privacy Service löst die Probleme des älteren Datenbrief-Konzeptes wie folgt. Durch die Nutzung der gleichen Zugangsdaten wie für den Internet-Dienst und die erforderliche Identifizierung nach dem Erhalt einer Benachrichtigung über die Erfassung besteht bei einer Fehladressierung kein Missbrauchspotential. Da die Datenbriefe nicht etwa elektronisch mittels E-Post zugestellt und somit zentralisiert gesammelt werden, schafft der dezentrale Abruf des Elektronischen Datenbriefes über einen standardisierten Elektronischen-Datenbrief-Dienst zudem keine weiteren potentiellen Angriffsziele. Zudem ist der Aufwand für die Internet-Dienstanbieter überschaubar, da durch die Integration des Elektronischen-Datenbrief-Dienstes in den bestehenden Internet-Dienst lediglich einmalige Kosten anfallen. Da dar Elektronischen-Datenbrief-Dienst standardisiert sein soll, bietet er eine sehr hohe Vertrauenswürdigkeit und Sicherheit.

# Umsetzung

## Überblick einer möglichen Umsetzung

Eine mögliche Umsetzung des Online Privacy Services (OPC) lässt sich wie folgt veranschaulichen:




Bei der Abbildung wird exemplarisch angenommen, dass Facebook (blau), Google (grün) und ein weiterer Dienst (orange) den Online Privacy Service (grau) implementieren.

### *Schichtenarchitektur*

Die verwendete Schichtenarchitektur erlaubt eine konzeptionelle Trennung des Modells, der Steuerung sowie Präsentation. Diese Strukturierung ist notwendig, da der Zugriff auf die Daten (Modell) von jedem Dienstanbieter verschieden implementiert werden muss und eine Darstellung der Daten (Präsentation) nicht nur im Browser sondern auch in weiteren Anwendungen ermöglicht werden soll (OPS App).

### *Implementierung*

Da die standardisierte Steuerungs- sowie Präsentationsschicht durch den Online Privacy Service zur Verfügung gestellt wird, ist auf Seiten der Dienstanbieter nur der Zugriff auf die Datenbank gegen die einheitliche Schnittstelle der Steuerungsschicht sowie ein Verweis auf die Präsentationsschicht in dem vorhandenen Dienst zu implementieren. Da die Steuerungs- sowie Präsentationsschicht physikalisch ebenfalls bei dem Dienstanbieter ausgeführt wird, benötigen diese Zugriffe auf den OPS Dienst um Aktualisierungen zu empfangen.

### *OPS-Dienst*

Der OPS-Dienst stellt Aktualisierungen der Steuerungs- und Präsentationsschicht zur Verfügung. Außerdem verwaltet er die Kategorisierung der Daten indem er kategorisierte Merkmale für allgemeine Daten anbietet und diese nach Anfragen der Dienstanbieter einheitlich ergänzt.

### *OPS-App*

Die OPS-App stellt die offizielle ebenfalls vom Online Privacy Service zur Verfügung gestellte Desktopanwendung dar. Über die einheitliche Schnittstelle der Steuerungsschicht kann diese die Daten der verschiedensten Dienstanbieter abrufen und ermöglicht dadurch eine globale Sicht und damit Vergleichbarkeit der Datensammlungen.

## Vorgehensweise zur Umsetzung

### *Standardisierung des Online Privacy Services*

Für die Standardisierung des Online Privacy Services empfiehlt sich die Einrichtung eines Arbeitskreises. Dieser sollte anschließend Rahmenbedingungen und eine Kategorisierung entwerfen.

Bei dem Entwurf der Kategorisierung muss beachtet werden, dass sich viele Daten der verschiedenen Dienste überschneiden. Somit besteht die Herausforderung darin, eine Kategorisierung zu entwerfen, die die Daten der verschiedenen Dienste genau einem Merkmal in der Kategorisierung zuordnet.

In einem weiteren Schritt müssen die standardisierte Steuerungs- und Präsentationsschicht sowie OPS-App entsprechend der erarbeiteten Rahmenbedingungen entwickelt werden. Aufgrund der Sensibilität der Daten ist bei der Entwicklung insbesondere auf höchste Sicherheitsvorkehrungen zu achten. Die entwickelte Software muss zudem entsprechend der Sicherheitsanforderungen zertifiziert werden.

### *Integration der Dienstanbieter*

Die Integration von Diensten verläuft typischerweise in den folgenden Schritten:

- Entwicklung der Modellschicht
- Beantragung neuer Merkmale
- Einbindung in die vorhandene Onlineplattform

Für die Entwicklung der Modellschicht muss den Dienstanbietern eine Dokumentation zu den Schnittstellen der Steuerungsschicht sowie Merkmalen der Kategorisierung zur Verfügung gestellt werden. Um Redundanzen zu vermeiden, muss außerdem die Zuordnung der Daten zu den Merkmalen der einheitlichen Kategorisierung während der Integration überprüft werden.

Für diesen Prozess muss es für den Dienstanbieter außerdem möglich sein, neue Merkmale in der Kategorisierung zu beantragen.

Die Einbindung in die vorhandene Onlineplattform muss vorgegebenen Rahmenbedingungen entsprechen, damit der Verweis zu dem Online Privacy Service von den Benutzern schnell und intuitiv gefunden werden kann.

### *Wartung des Online Privacy Service*

Die Wartung des Online Privacy Services muss die mindestens monatliche Aktualisierung der Kategorien und Merkmale umfassen. Außerdem muss die standardisierte Steuerungs- und Präsentationsschicht kontinuierlich weiterentwickelt und in Zuge dessen der aktuellen Sicherheitslage angepasst werden.

### *Betreuung durch die Dienstanbieter*

Die Dienstanbieter müssen nach der Integration verpflichtet sein, Anfragen, die über den Online Privacy Service eingehen, in einem vorgeschriebenen Zeitraum individuell zu bearbeiten.

# Prototyp

## Facebook als Datenquelle

Der Prototyp wurde als eine fiktive Integration in Facebook entwickelt, da für diesen Dienst weitgehende bereits anonymisierte Datensätze über das Projekt europe-v-facebook.org von Max Schrems zur freien Verfügung stehen. Dieser hatte im Juni 2011 seine persönlichen Daten bei Facebook angefordert und daraufhin ein 1.222 Seiten umfassendes Dokument von Facebook erhalten. Die darin enthaltenen 57 Datensätzen gliedern sich in 22 Datensätze mit Profilinformationen sowie 35 Datensätze mit generierten Daten.

Durch den hohen Zuwachs an Anfragen durch die Initiative von Schrems, ist ein Datendownload seit November 2011 bei Facebook möglich. Dieser enthält jedoch lediglich die Profilinformationen, was eine Irritation des Benutzers darstellt, da keine volle Dateneinsicht erfolgt. Beispielsweise sind keine über den Benutzer generierten Daten enthalten.

## Kategorisierung

Mit der Erstellung des Prototyps war gleichzeitig der Entwurf einer Kategorisierung notwendig. Die entwickelte Kategorisierung kann alle Daten des anonymisieren Facebook Datensatzes von Schrems aufnehmen, stellt durch die Wahl von allgemeingültigen Kategorisierungen und Merkmalen jedoch ein generisches Modell dar, sodass dieses auch für weitere Dienste verwendet werden kann.

Die Google Dienste lassen sich beispielsweise wie folgt in das generische Modell einordnen:

- +1 in *Vorlieben und Gefühle*
- Circles in *Kontakte*
- Google Buzz in *Kommunikation*
- Kontakte in *Kontakte*
- Picasa-Webalben in *Multimedia*

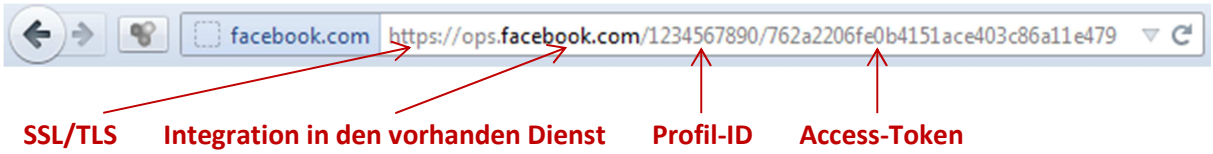
Und auch die Daten eines weniger verwandten Anbieters wie einer Krankkasse lassen sich in das generische Modell einordnen. Dabei würden die spezifischeren Daten in einer bei dem Online Privacy Dienst zu beantragenden neuen Kategorie *Gesundheit* Platz finden.

## Integration

Die Einbindung in die vorhandene Onlineplattform am Beispiel Facebook könnte wie folgt aussehen:


Dabei wäre gewährleistet, dass der Verweis zu dem Online Privacy Service schnell und intuitiv zu finden ist.

Der Verweis könnte beispielsweise wie folgt realisiert werden:

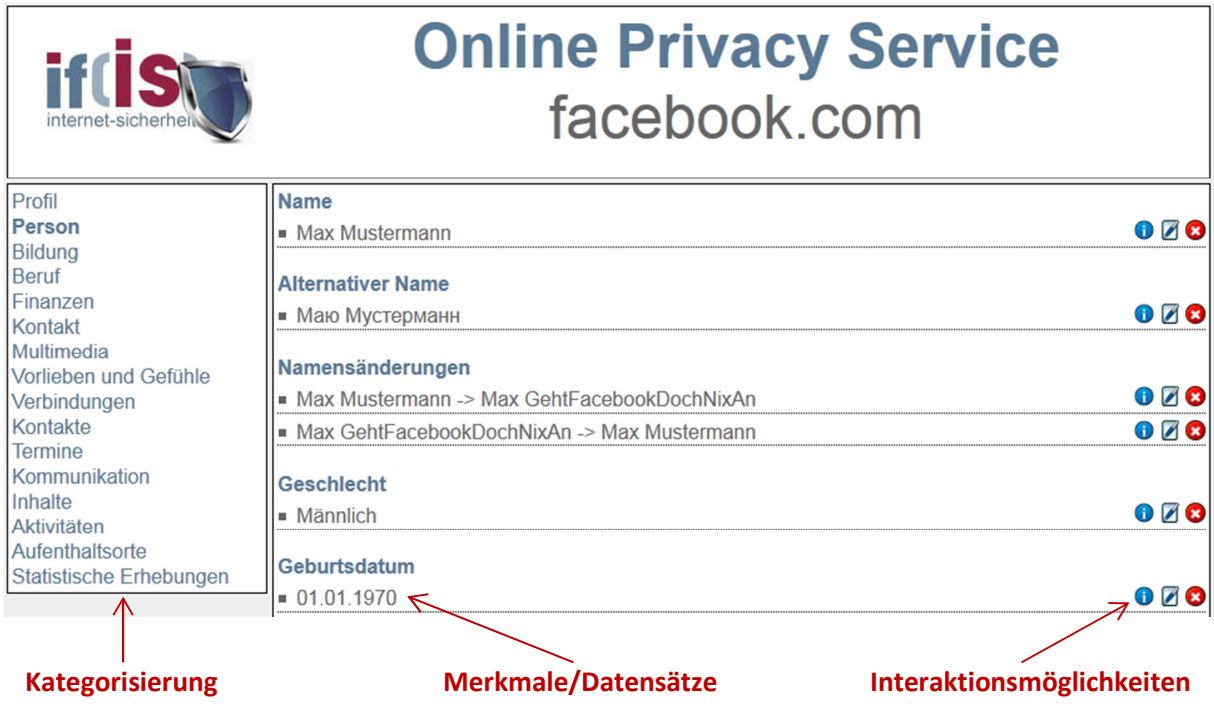



Dabei realisiert SSL/TLS eine sichere Verbindung zu dem Online Privacy Service. Durch die Verwendung eines Access-Tokens kann nur die zu dem Access-Token passende Profil-ID aufgerufen werden.

Zusätzlich könnte durch ein IP-Binding, die Versendung einer Mobil-TAN (Medienwechsel) sowie eine Verifikation durch den neuen Personalausweis eine noch stärkere Sicherheit gewährleistet werden.

## Einheitliche Ansicht

Die einheitliche Ansicht wurde in dem Prototypen wie folgt realisiert:




Dabei ist zu beachten, dass es sich bei dem Entwurf des Prototyps lediglich um eine Veranschaulichung einer möglichen Umsetzung handelt und kein Wert auf ein ansprechendes Design gelegt wurde.

## Interaktionsmöglichkeiten

Um dem Benutzer die Möglichkeit zu geben sich weitere Informationen zu den Merkmalen anzeigen zu lassen oder Rückfragen zu Merkmalen zu stellen, wurden die folgenden Interaktionsmöglichkeiten integriert:

- Informationen
- Korrektur beantragen
- Löschung beantragen

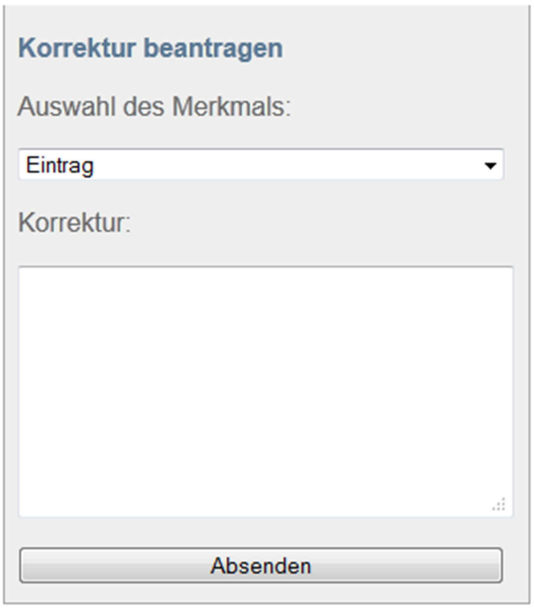
Diese Interaktionsmöglichkeiten lassen sich bequem in einem Pop-Up-Fenster benutzen.

### *Informationen*


Das Fenster *Informationen* liefert die folgenden ergänzenden Informationen zu einem Merkmal:

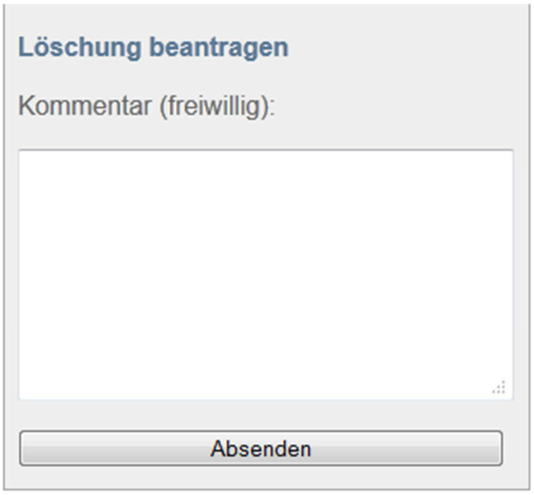
- Zeitpunkt der Speicherung
- Ursprung der Daten
- Zweck der Speicherung
- Übermittlung der Daten
- Rechtsgrundlage der Übermittlungen

### *Korrektur beantragen*




Das Fenster *Korrektur beantragen* bietet die Möglichkeit, die verschiedenen Informationen des Merkmals zu korrigieren. Nach dem Absenden der Korrektur geht diese bei dem entsprechenden Dienstanbieter ein, um anschließend zeitnah in einem vorgeschriebenen Bearbeitungszeitraum überprüft zu werden.

### *Löschung beantragen*




Das Fenster *Löschung beantragen* bietet die Möglichkeit, die Inhalte eines kompletten Merkmals zu löschen. Nach dem Absenden der Löschung geht diese ebenfalls bei dem entsprechenden Dienstanbieter ein, um anschließend zeitnah in einem vorgeschriebenen Bearbeitungszeitraum überprüft zu werden.

Weitere Information siehe:

Mit dem folgenden Link können Sie sich ein Bild von einer möglichen Realisierung machen (Web-Oberfläche):

http://www.internet-sicherheit.de/temp/ops/

Artikel und Vortrag: Elektronischer Datenbrief

http://www.internet-sicherheit.de/institut/forschung/publikationen-vortraege/dokumente-als-pdfs/dokumente-2012/?no_cache=1&tx_damfrontend_pi1%5Bpointer%5D=1