Privacy by Design: Wunschvorstellung oder Qualitätsmerkmal?

Entwicklertag

Karlsruhe, 15.06.2016

DRUCKVERSION

Christoph Schäfer

secorvo
security consulting

Agenda

(1) Datenschutz

(2) Gesetzliche Regelungen

(3) (Negative) Beispiele

(4) Lösungsansätze

(5) Best practice

(6) Fazit

Datenschutz?

Besondere personenbezogene Daten

Name

Adresse

Finanzielle Situation

Gewerkschafts-zugehörigkeit

Fotos

Gesundheit

Religion

Autokenn-zeichen

Hobbies, Freunde

Geburts-datum

Familien-stand

Politische Ansichten

Ethnische Herkunft

Sexuelle Vorlieben

Nutzerdaten (GPS, Surfen, Telefon)

Datenschutz = Schutz von Daten?

Wem gehören die Daten?

§ 903 BGB – Befugnisse des Eigentümers

Der Eigentümer einer Sache kann, soweit nicht das Gesetz oder Rechte Dritter entgegenstehen, mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen. (…)

Besser:
Wer darf die Daten für welche(n) Zweck(e) nutzen?

Gesetzliche Regelungen

Bundesdaten-schutzgesetz (BDSG)

Datensparsamkeit*

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

* § 3a BDSG

Sammelbilder von Rewe

Mittwoch, 20.07.2011, 11:41

Hacker veröffentlichen Kundendaten im Internet

Rewe ist Opfer eines Hackerangriffs geworden dpa

Die Daten der Rewe-Sammelbörse sind nicht nur kopiert worden. Die Hacker haben sie nun auch im Netz veröffentlicht. Wer sein E-Mail-Passwort nicht geändert hat, muss mit unangenehmen Folgen rechnen.

Nach dem **Hackerangriff auf die Sammelbild-Tauschbörsen** des Handelskonzerns Rewe haben Unbekannte Zehntausende Kundendaten im Internet veröffentlicht. „Es wurde gestern eine signifikant hohe Anzahl unserer Daten ins Netz gestellt", sagte ein Rewe-Sprecher am Mittwoch in Köln. Es handle sich um E-Mail-Adressen und dazu gehörende Passwörter von bis zu 45 000 Kunden. Diese hatten sich mit den Daten auf einer Rewe-Seite angemeldet, um Tier- oder Fußballbilder zu tauschen. Zunächst hatte es geheißen, es sei unklar, ob die Daten kopiert worden seien.

sueddeutsche.de

22.07.2011 um 14:39 Uhr

Nach Hackerangriff: Rewe will Sicherheit verbessern

Köln (dpa) - Zehntausende Sammelfreunde sind von dem Hackerangriff bei Rewe betroffen. Nun kündigt das Unternehmen einen besseren Schutz von Kundendaten an. Datenschutzbehörden verlangen von Rewe schriftliche Antworten auf offene Fragen.

«Meine Mitarbeiter haben einen Kontrollbesuch gemacht. Dabei ist eine ganze Reihe von Fragen noch nicht zu meiner Zufriedenheit geklärt worden», sagte der NRW-Landesbeauftragte für Datenschutz, Ulrich Lepper, der «Bild»-Zeitung. Seine Sprecherin erläuterte, es sei zum Beispiel nicht ersichtlich, warum jemand, der an der Sammelbörse teilnimmt, seine Postadresse angeben solle. Auch die vertraglichen Regelungen zwischen Rewe und dem Dienstleister, der die Datenbank erstellt hat, seien der Datenschutzbehörde noch unklar. «Wir werden die Antworten auf unsere Fragen jetzt schriftlich anfordern», sagte die Sprecherin in Düsseldorf.

Sanktionen gem. BDSG

- Bis zu 300.000 € Bußgeld (je Verstoß)
- Gewinnabschöpfung
- Bis zu 2 Jahre Haft (bei Vorsatz)
- Schadensersatzanspruch

Verstoß gegen Datensparsamkeit:

0,00 €

EU-Datenschutz-grundverordnung

(ab Mai 2018)

Artikel 25: Data protection by design and by default

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung —, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Artikel 25: Data protection by design and by default

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.
(…)

EU-DSGVO – Erwägungsgrund 78

- Verarbeitung personenbezogener Daten minimieren
- So schnell wie möglich pseudonymisieren
- Funktionen und Verarbeitung transparent machen
- Betroffenen Überwachung ermöglichen
- Sicherheitsfunktionen vorsehen

(…)

„Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen **sollte** auch bei öffentlichen Ausschreibungen Rechnung getragen werden.“

EU-DSGVO – Erwägungsgrund 78

(…) In Bezug auf **Entwicklung**, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, **sollten** die **Hersteller** der Produkte, Dienste und Anwendungen **ermutigt werden**, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.
(…)

Verstoß gegen Datensparsamkeit*:

0,00 €

* Alt, bis 04/2018

Verstoß gegen Data protection by design and by default*:

bis 10 Mio € oder 2 % des weltweiten Jahresumsatzes

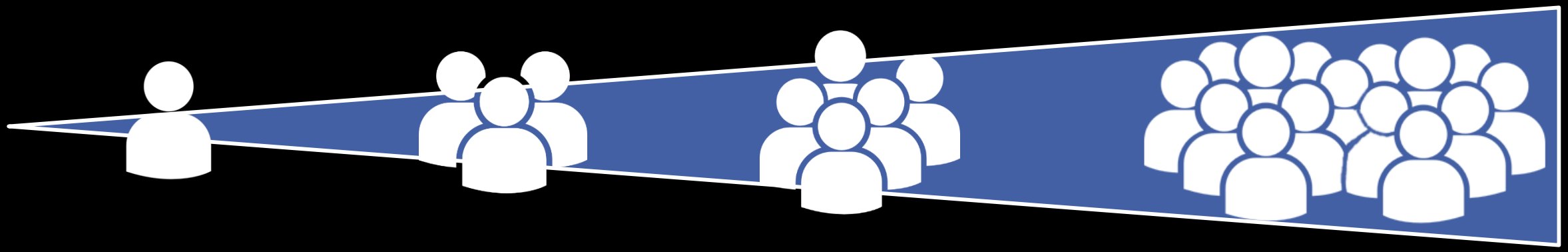
(je nachdem, welcher der Beträge höher ist)

* Neu, ab 05/2018

(Negative) Beispiele

Privacy by DESIGN

Facebook Privatsphäre-Einstellungen



Nur ich | Listen | Freunde | Öffentlich

Wie können wir dir helfen?

Desktop-Hilfe
Deutsch

Anmeldung und Passwort
Erste Schritte bei Facebook
Verwalte dein Konto
Privatsphäre
Sicherheit
Neuigkeiten
Geteilte Inhalte
Nachrichten
Verbindungen
Seiten
Werbeanzeigen

Welche Namen sind auf Facebook zugelassen?

Facebook ist eine Gemeinschaft, in der die Menschen ihre authentischen Identitäten verwenden. Es ist erforderlich, dass alle Menschen ihren echten Namen angeben, damit immer klar ist, mit wem du dich verbindest. Das trägt zur Sicherheit unserer Gemeinschaft bei.

Folgende Elemente darfst du deinem Namen nicht hinzufügen:

- Symbole, Nummern, ungewöhnliche Großschreibung, sich wiederholende Zeichen oder Satzzeichen
- Zeichen aus verschiedenen Sprachen
- Titel jeglicher Art (z. B. beruflich, religiös)
- Wörter oder Formulierungen anstelle des mittleren Namens
- Beleidigende oder anstößige Wörter jeglicher Art

Zudem gelten folgende Richtlinien:

- Bei dem Namen, den du verwendest, muss es sich um den Namen handeln, mit dem dich deine

Donnerstag, 03.03.2016 – 18:04 Uhr

Klarnamen-Pflicht: Facebook wehrt Forderung von Datenschützern ab

SPIEGEL ONLINE

Facebook-Logo in der Zentrale in Dublin

Nutzer müssen sich weiterhin mit ihrem echten Namen bei Facebook anmelden. Ein Gericht stoppte Pläne von Hamburgs oberstem Datenschützer. Er wollte Facebook zwingen, auch Pseudonyme zuzulassen.

§ 13 TMG*: Pflichten des Diensteanbieters

- (…)
- (6) Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.
- (…)

- * Telemediengesetz

36. Tätigkeitsbericht (2007)

5.10.3.2 Löschung von Daten im SAP R/3 HR-System

(…)

Die Löschung von Daten ist im SAP-Standard nicht vorgesehen.

(…)

Ich werde die Umsetzung der Löschkonzepte zeitnah und konkret überprüfen. Ein SAP-System, das die Daten, wie gesetzlich vorgeschrieben, nicht rechtzeitig und umfassend löscht, ist datenschutzrechtlich zu beanstanden. (…)

41. Tätigkeitsbericht (2012)

3.3.6.1 Löschen von Daten im SAP R/3 HR-System

(…)

hatte ich über den Sachstand zur Löschung von Krankheits- und Urlaubsdaten im SAP R/3 HR-System, die am 31. Dezember 2006 schon hätten gelöscht sein müssen, berichtet. Es handelte sich um 7.559 Datensätze. (…)

Eine erneute Überprüfung der Löschpraxis im SAP R/3 HR-System hat ergeben, dass auch am 1. Oktober 2012 noch immer 2.968 Datensätze aus diesem Zeitraum nicht gelöscht waren.

(…)

42. Tätigkeitsbericht (2013)

5.1.1 Löschen von Abwesenheiten

(…)

Leider musste ich jetzt feststellen, dass (…) die Löschung (…) immer noch nicht konsequent durchgeführt wird: Eine Auswertung zum Stichtag 14.11.2013 hat ergeben, dass wiederum 2.834 löschbare Fälle nicht bearbeitet wurden. Die Gründe hierfür kann ich nicht nachvollziehen.

(…)

5.1.2 Löschung ganzer Datensätze

Das Programm zum „Löschen ganzer Datensätze“ im SAP R/3 HR-System wurde im Frühjahr 2013 fertig gestellt und produktiv gesetzt.

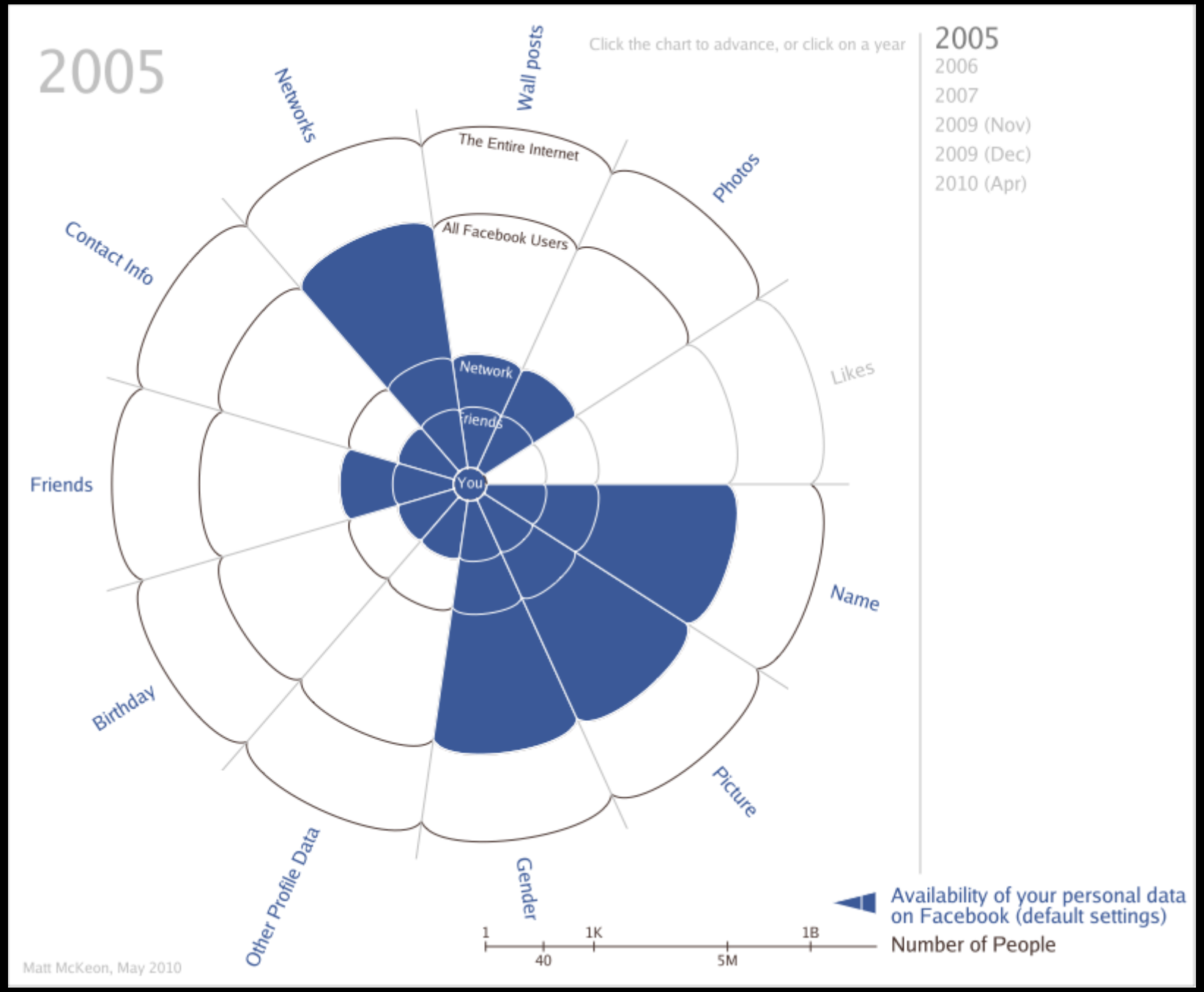
Datenvernichtung im HR

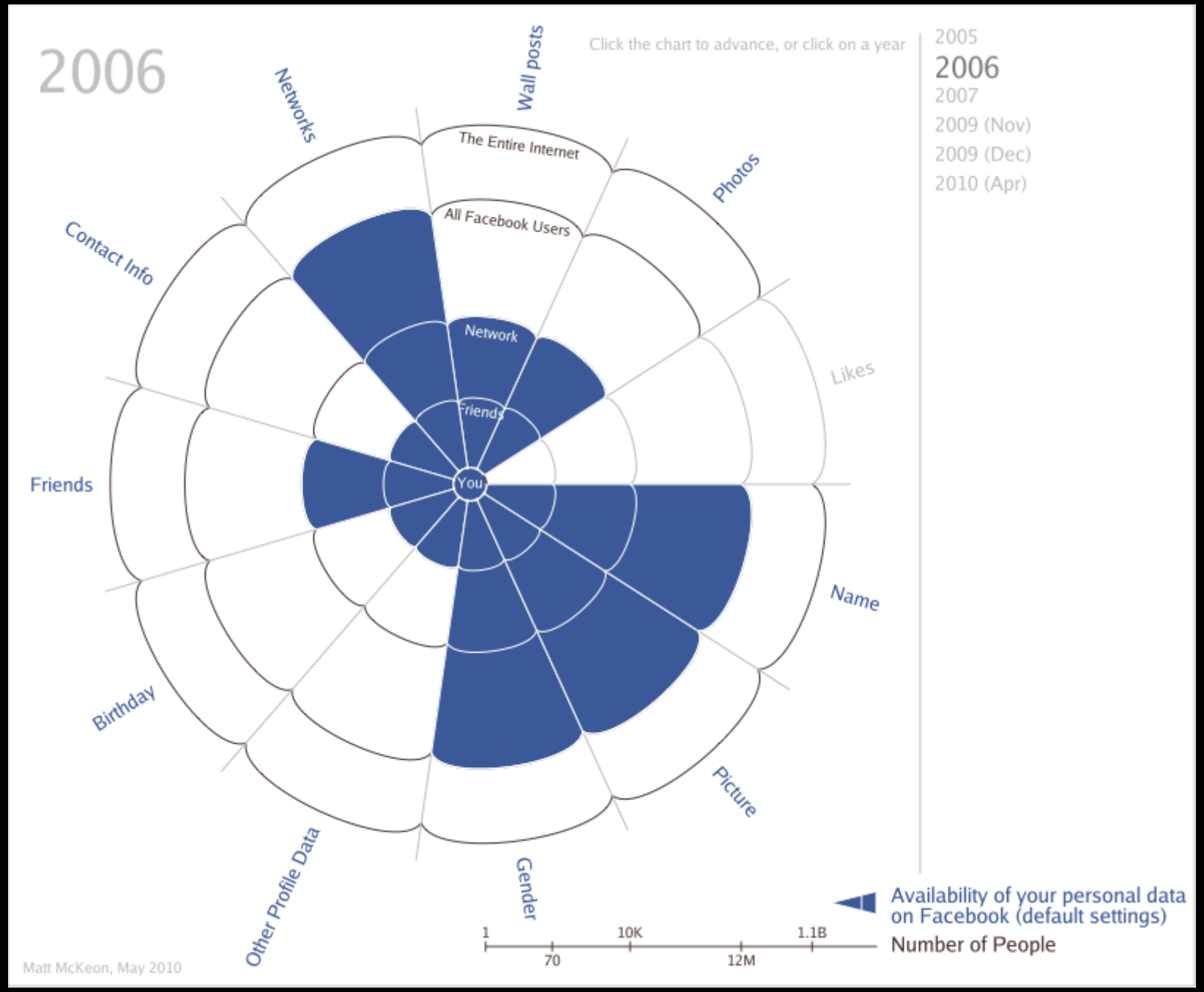
Mit der Datenvernichtung des SAP NetWeaver Information Lifecycle Management (ILM) können Sie personenbezogene Stammdaten aus Anwendungen der Personalwirtschaft (HR) nach Ablauf der dafür festgelegten Aufbewahrungsdauer vernichten. Wenn die Aufbewahrungsregeln für die Daten erfüllt sind, löscht das System die Daten vollständig aus dem operativen System und dem Archivsystem.

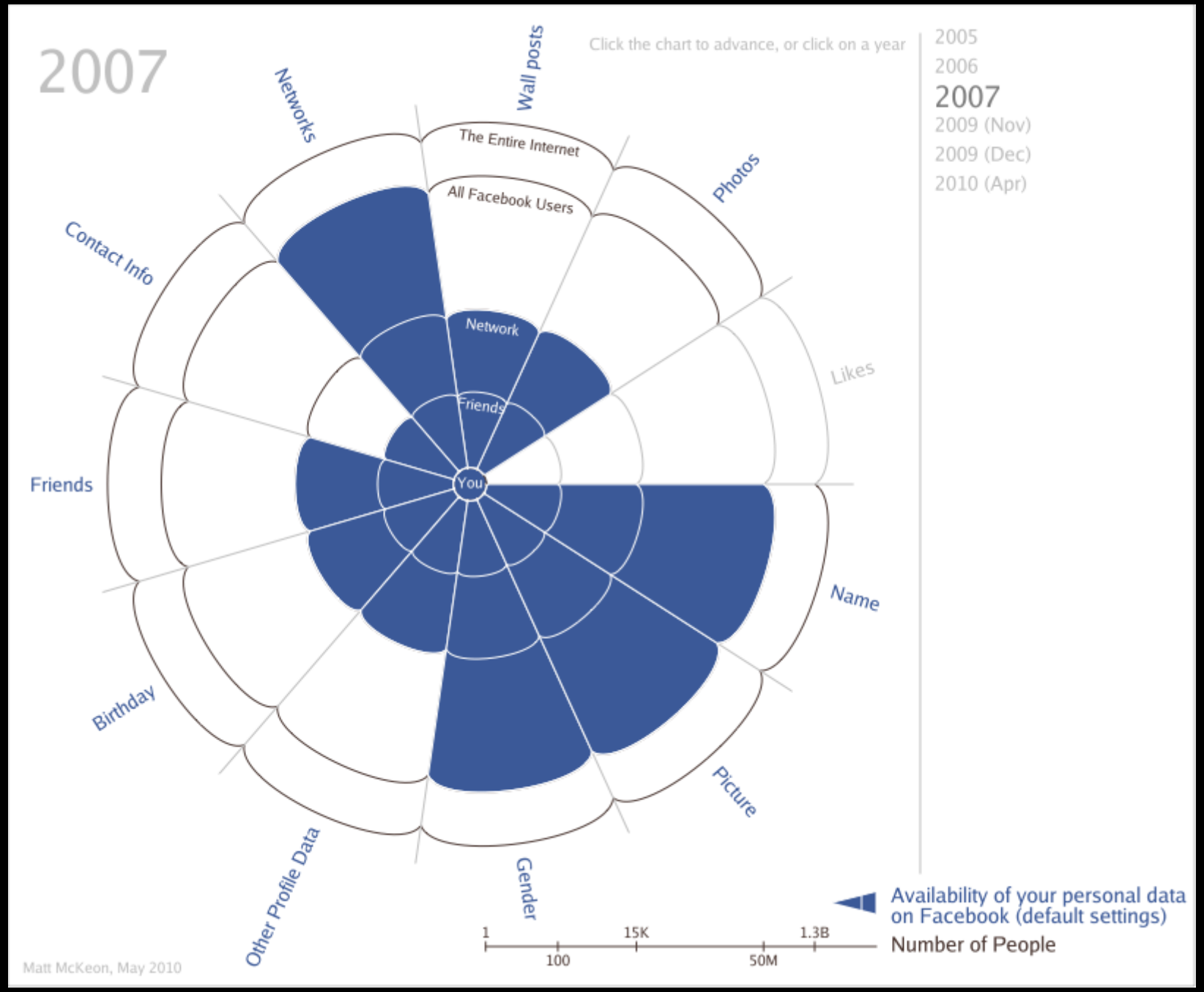
Achtung

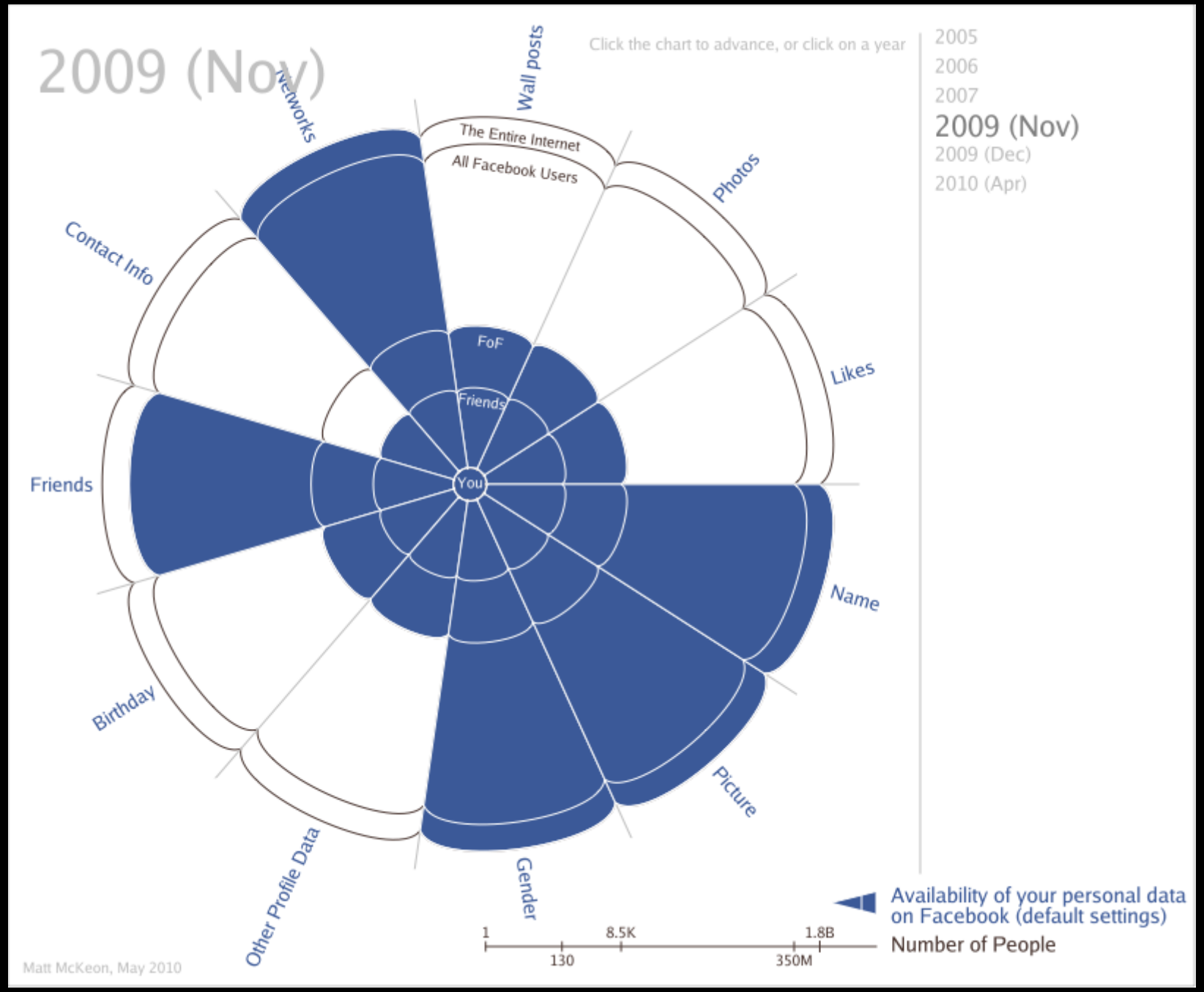
Die Datenvernichtung ist nach der Löschphase irreversibel.

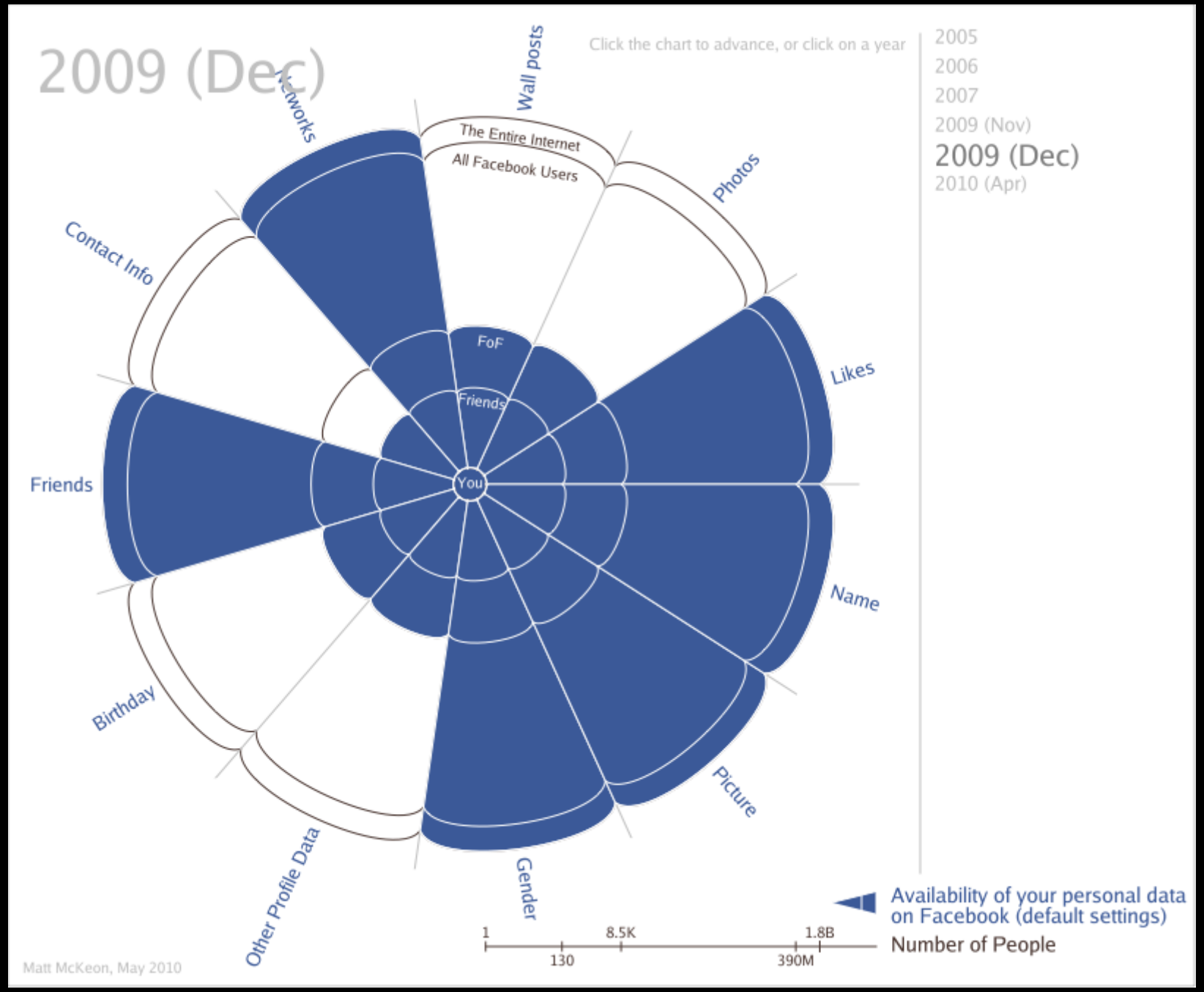
…and by DEFAULT?

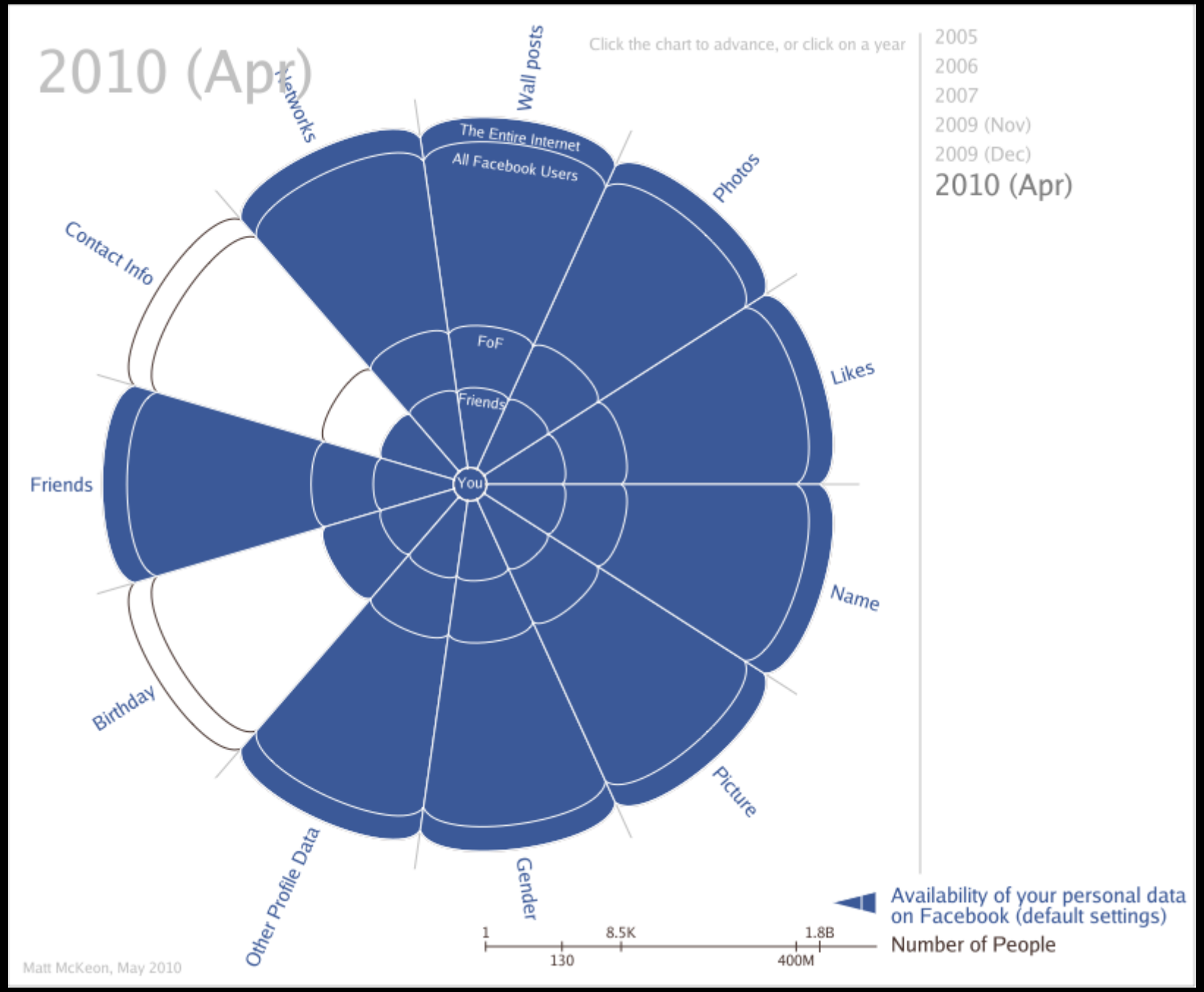












RP ONLINE

Grenoble/Düsseldorf

Klinik sperrt Schumachers Krankenakte

11. Januar 2014 | 10.50 Uhr

Grenoble/Düsseldorf. Der gesundheitliche Zustand von Michael Schumacher ist auch 13 Tage nach seinem schweren Ski-Unfall in der Schweiz weiter kritisch, aber stabil. Unterdessen hat die Uni-Klinik im französischen Grenoble, wo der ehemalige Formel-1-Weltmeister behandelt wird, die Einsicht in Schumachers Patientenakte gesperrt. Nach Informationen der "Bild" konnte zuvor jeder der über 1600 Krankenhaus-Mitarbeiter per Computer Informationen über das aktuelle Befinden des 45-Jährigen einholen. Auch die Scans von Schumachers Gehirn sollen vielfach aufgerufen worden sein. Die Aufforderungen der Klinikleitung, dies zu unterlassen, seien ignoriert worden. Nun ist die Akte gesperrt.

heise Security

WhatsApp: Verschlüsselung für alle freigeschaltet

05.04.2016 18:43 Uhr – Ronald Eikenberg

WhatsApp verschlüsselt ab sofort sämtliche Kommunikation auf allen Plattformen, wenn beide Gesprächspartner die aktuelle Version installiert haben. Damit wird WhatsApp auf einen Schlag zum meistgenutzten Krypto-Messenger.

Lösungsansätze

IPC Ontario

OECD

ETTER POLICIES FOR BETTER LIVE

OECD

enisa

European Network and Information Security Agency

ENISA

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

DSB-Konferenz

secorvo
security consulting

IPC of Ontario: Privacy by Design*

1. Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe
2. Datenschutz als Standardeinstellung („Privacy by Default“)
3. Der Datenschutz ist in das Design eingebettet
4. Volle Funktionalität – eine Positivsumme, keine Nullsumme
5. Durchgängige Sicherheit – Schutz während des gesamten Lebenszyklus
6. Sichtbarkeit und Transparenz – Für Offenheit sorgen
7. Die Wahrung der Privatsphäre der Nutzer – für eine nutzerzentrierte Gestaltung sorgen

* von Ann Cavoukian, ehem. Information and Privacy Commissioner, Ontario (Canada), in 2010 als globaler Standard von der internat. Konferenz für Datenschutz festgelegt

OECD Privacy Principles*

1. Begrenzte Datenerhebung
2. Datenqualität
3. Zweckbestimmung
4. Nutzungsbegrenzung
5. Sicherheit
6. Transparenz
7. Mitspracherecht
8. Rechenschaftspflicht

* Organization for Economic Cooperation and Development (OECD), Original von 1980, aktualisiert 2015

ENISA: Privacy and Data Protection by Design*

Technische Prinzipien

1. MINIMISE — Datensparsamkeit als Prämisse
2. HIDE — Verbergen um vor Missbrauch zu schützen
3. SEPARATE — Daten aufteilen und getrennt ablegen
4. AGGREGATE — Anonymität in der Masse, Beschränkung der Details

Organisatorisch Prinzipien

5. INFORM — Transparenz gegenüber Betroffenen
6. CONTROL — Kontrollmöglichkeiten durch den Betroffenen
7. ENFORCE — Konzepte/Dokumentationen sind zugänglich
8. DEMONSTRATE — Nachweisen, dass man sich an Konzepte hält

* Europäischen Agentur für Netz- und Informationssicherheit (ENISA), Empfehlung vom Januar 2015

Standard-Datenschutzmodell (SDM), V.0.9*

1. Datensparsamkeit
2. Verfügbarkeit
3. Integrität
4. Vertraulichkeit
5. Nichtverkettbarkeit
6. Transparenz
7. Intervenierbarkeit

* Empfehlung der 90. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom Oktober 2015

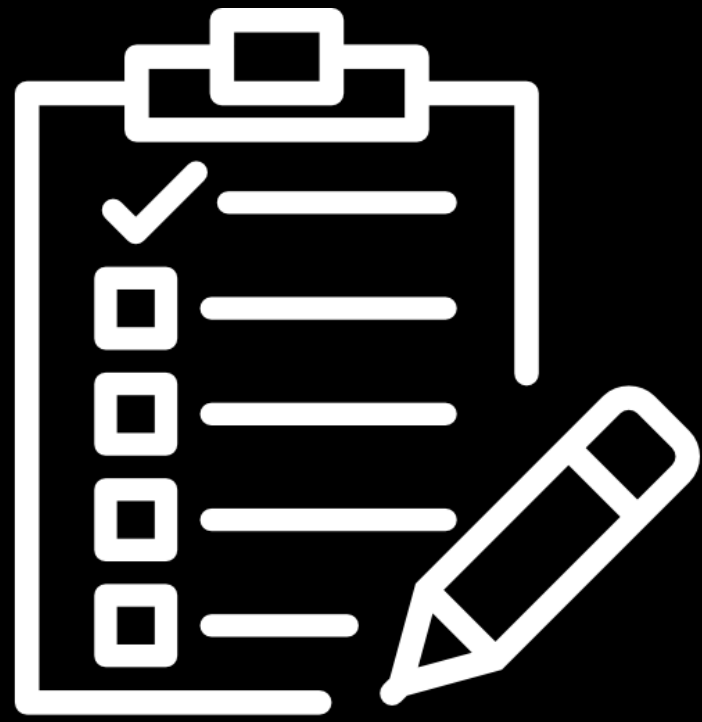
Außerdem …

OWASP Top 10 Privacy Risks*

1. Schwachstellen in Web-Applikationen
2. Datenabfluss beim Betreiber
3. Unzureichende Reaktion bei einer Datenpanne
4. Unzureichende Löschung personenbezogener Daten
5. Intransparente Nutzungsbedingungen
6. Sammeln von Daten, die über den eigentlichen Zweck hinaus gehen
7. Weitergabe von Daten an Dritte
8. Veraltete personenbezogene Daten
9. Fehlendes oder unzureichendes Session-Ende
10. Unsichere Datenübertragung

* Top 10 Datenschutz-Risiken in Web-Anwendungen und Gegenmaßnahmen, Version 1, September 2014

ISO/IEC 27018:2014 – Datenschutz für Cloud-Betreiber



ISO 27018 **ISO 27002**

Best practice

… gibt es leider kaum.

Compliance-Design-Prinzipien*

* Projektarbeit Secorvo

Security-Design-Prinzipien

(42 Controls)

+

Datenschutz-Design-Prinzipien

(50 Controls + 25 für Cloud/Dienstleister)

42 Controls

Security-Design-Prinzipien (SDP)

S	T	R	I	D	E	Kategorien	ID	Design-Prinzipien	Anmerkungen	Referenzen auf SDP in der Literatur	Referenzen auf ISO 27001 Kontrollen
x	x	x	x	x	x	**Sichere Anwendungs-entwicklung**	**SDP9.1**	Wir verfügen über Entwicklungsrichtlinien und kontrollieren ihre Einhaltung.	Entwicklungsrichtlinien beinhalten bspw. Secure Coding Guidelines. Entwickler sind darüber zu schulen.	Security Design Assurane	A.14.2.1 Secure development policy
	x					Sichere Anwendungs-entwicklung	**SDP9.2**	Veränderungen an Software sind auf die notwendigen Änderungen zu begrenzen. Alle Änderungen sind zu kontrollieren.	Sicherheitsschwachstellen können durch unkontrollierte Änderungen verursacht werden.		A.14.2.4 Restrictions on changes to software packages
	x		x			Sichere Anwendungs-entwicklung	**SDP9.3**	Wir nutzen eine geschützte Entwicklungsumgebung, die Zugriffskontrollen für den gesamten ebenszyklus der Systementwicklung und -integration vorsieht.	z. B. Zugriffskontrolle für Quellcode		A.14.2.6 Secure development environment A.9.4.5 Access control to program source code

50 Controls + 25 für Cloud/DIenstleister

Datenschutz-Design-Prinzipien (DDP)

Kategorien	ID	Design-Prinzip	Anmerkungen	SDP-Relevanz	SDP-Bezug	Normen-Bezug
Nichtverkettbarkeit	DDP5.01	Wir schränken Verarbeitungs-, Nutzungs- und Übermittlungsrechte ein.		Voll erfüllt durch	SDP2.3	Anlage zu § 9 Satz 1 Nr. 3 BDSG
Nichtverkettbarkeit	DDP5.02	Wir setzen auf eine programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und	Die Vorgabe Entwicklungsrichtlinien vorzugeben umfasst nicht spezifisch die Schnittstellenschließung	Teilweise erfüllt durch	SDP9.1	Anlage zu § 9 Satz 1 Nr. 3-5 BDSG
Nichtverkettbarkeit	DDP5.03	Wir etablieren regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur	Die Vorgabe Entwicklungsrichtlinien vorzuhalten enthält nicht spezifisch das Verbot von Backdoors	Teilweise erfüllt durch	SDP9.1	Anlage zu § 9 Satz 1 Nr. 3-4 BDSG
Nichtverkettbarkeit	DDP5.04	Wir trennen nach Organisations-/Abteilungsgrenzen, mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die	Die Aufteilung von Berechtigungen kann auch die Trennung nach Organisationsgrenzen erfassen. Sie zielt aber nicht auf die organisatorische Trennung mit Blick auf die datenschutzrechtliche Zweckbindung.	Teilweise erfüllt durch	SDP2.4	§ 5 BDSG, Anlage zu § 9 Satz 1 Nr. 3 BDSG
Nichtverkettbarkeit	DDP5.05	Wir ermöglichen nutzerkontrolliertes Identitätsmanagement durch die verarbeitende Stelle.				Anlage zu § 9 Satz 1 Nr. 3, 5 BDSG
Nichtverkettbarkeit	DDP5.06	Wir setzen durch zweckspezifischen Pseudonyme, Anonymisierungsdienste und anonyme Credentials nach Möglichkeit				§ 3a BDSG
Nichtverkettbarkeit	DDP5.07	Wir sehen Verfahren vor, die bei der Veränderung von Verarbeitungszwecken zu einer erneuten Datenschutzprüfung führen.				§ 4 Abs. 1 und Abs. 3 Nr. 2 BDSG

ZEIT ONLINE

14. Juni 2016, 21:57 Uhr

Privatsphäre

Apples heilige Kuh auf dünnem Eis

An Nutzerdaten hat Apple kein Interesse, betont das Unternehmen stets. Nun könnte es den Grundsatz aufweichen. "Differential Privacy" soll Apples Technik schlauer machen.

Von **Patrick Beuth**, San Francisco

Apples Craig Federighi erklärte auf der WWDC, warum sein Unternehmen künftig Nutzerdaten sammelt, um sie auszuwerten. © Stephen Lam/Reuters

Heilige Kühe darf man nicht töten, schon klar. Aber ist es okay, wenn man sie ein bisschen schubst? Vor dieser Frage steht Apple gerade, im übertragenen Sinn natürlich.

Differential Privacy

Das Prinzip von „Differential Privacy“ gibt es schon lang. Wissenschaftler wollen bei Umfragen durchgehende wahrheitsgemäße Beantwortung gewährleisten, auch wenn diese z. B. peinlich wäre. Deshalb ließen Forscher die Probanden eine Münze werfen. Zeigte sie Kopf, lautete die Antwort automatisch "Ja", unabhängig davon, ob sie stimmte. Zeigte sie aber Zahl, mussten die Probanden wahrheitsgemäß antworten. Das ermöglichte jedem Einzelnen im Nachhinein, zu bestreiten, wirklich "Ja" gemeint zu haben - schließlich wurde statistisch gesehen die Hälfte von ihnen von der Münze dazu gezwungen. Statistisch gesehen landet eine Münze bei 1000 Würfen 500-mal auf dem Kopf. Dadurch lässt sich errechnen, wie viele der Ja-Antworten tatsächlich der Wahrheit entsprechen.

Fazit: Wunschvorstellung oder Qualitätsmerkmal?

Volkszählungsurteil (15.12.1983)

Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.

DESIGN + DEFAULT!

Probleme der Ansätze

Wie konkret umsetzen?

Woher Werkzeuge nehmen?

Woher Best practice nehmen?

Wer ist verantwortlich?

Was ist noch zu beachten?

Wie mit werbefinanzierten Diensten übereinkommen?

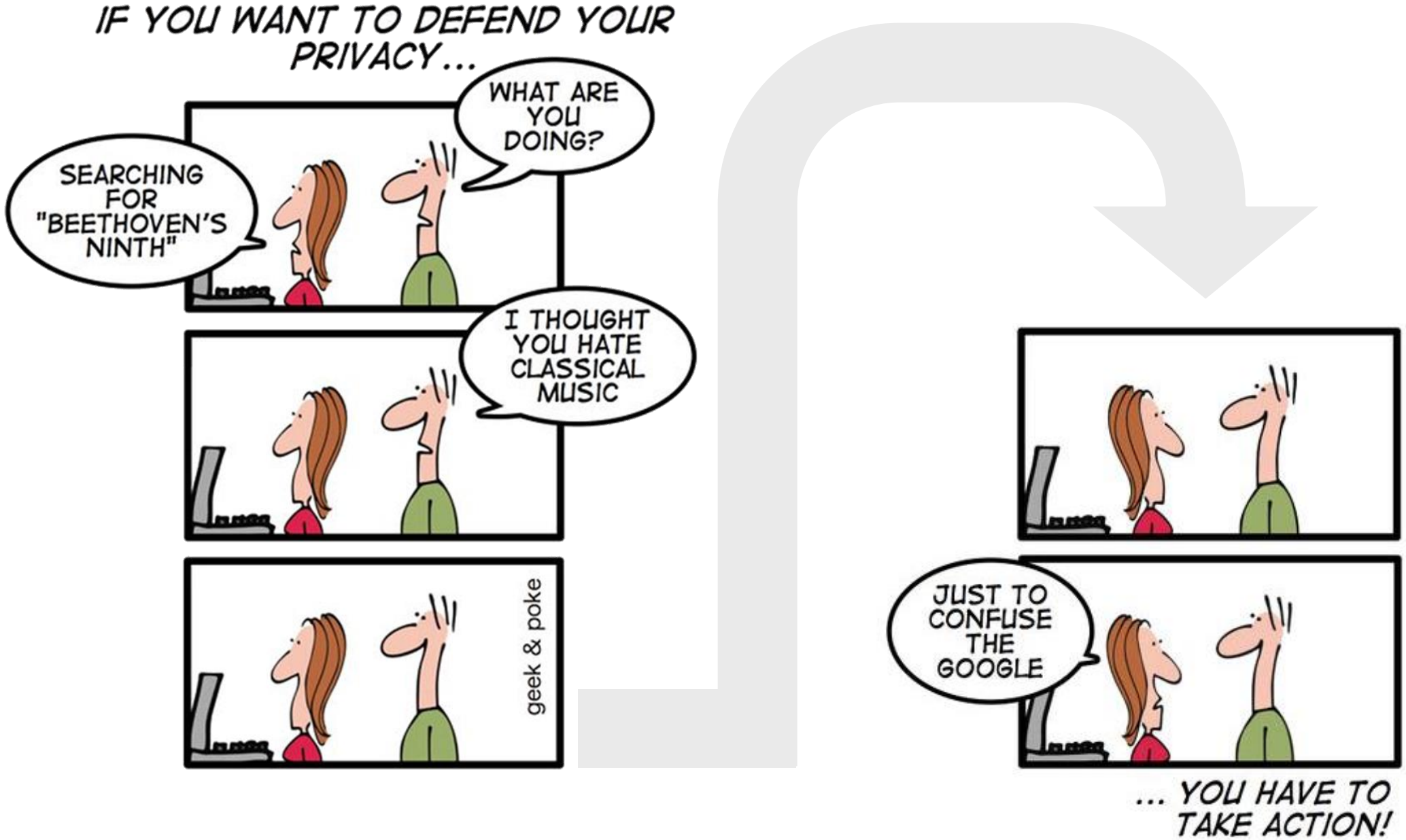
Wer trägt Kosten?

NETZPOLITIK.ORG

Apples „Differential Privacy“: Privatsphäre als Verkaufsargument

von Constanze am 14. Juni 2016, 15:42 in Technologie / 8 Kommentare

Bei der gestrigen Apple-Show WWDC zeigte sich ein Trend: Der Konzern stellte mehrere technische Lösungen vor, die den Schutz der Privatsphäre der Nutzer in den Vordergrund stellen. Im hochpreisigen Marktsegment stellt sich Apple in Sachen Datenschutz weiterhin klar gegensätzlich zu Google oder Microsoft auf.




TOP
CONSULTANT
IT-Berater
2015
secorvo
security consulting
Ettlinger Str. 12-14
76137 Karlsruhe
Telefon +49 721 255171-0
Telefax +49 721 255171-100
info@secorvo.de
www.secorvo.de