ÖFIT-Trendschau

Öffentliche Informationstechnologie in der digitalisierten Gesellschaft

Trendthema 10:

Post Privacy

Stand: Juli 2016

Herausgeber:
Mike Weber
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut FOKUS
Kaiserin-Augusta-Allee 31, D-10589 Berlin
Telefon: +49 30 3463 - 7173
Telefax: + 49 30 3463 - 99 - 7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

Autorinnen und Autoren der Gesamtausgabe:
Mike Weber, Stephan Gauch, Faruch Amini, Tristan Kaiser, Jens Tiemann, Carsten Schmoll, Lutz Henckel, Gabriele Goldacker, Petra Hoepner, Nadja Menz, Maximilian Schmidt, Michael Stemmer, Florian Weigand, Christian Welzel, Jonas Pattberg, Michael Rothe, Oliver Schmidt, Nicole Opiela, Florian Friederici, Jan Gottschick, Jens Fromm

Autorinnen und Autoren einzelner Trendthemen:
Michael Rothe, Oliver Schmidt

ISBN: 978-3-9816025-2-4

Juli 2016

Autorinnen/Autoren:
Mike Weber et al.

Bibliographische Angabe:
Mike Weber et al. 2019, Post Privacy, In: Jens Fromm und Mike Weber, Hg., 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT., http://www.oeffentliche-it.de/-/post-privacy

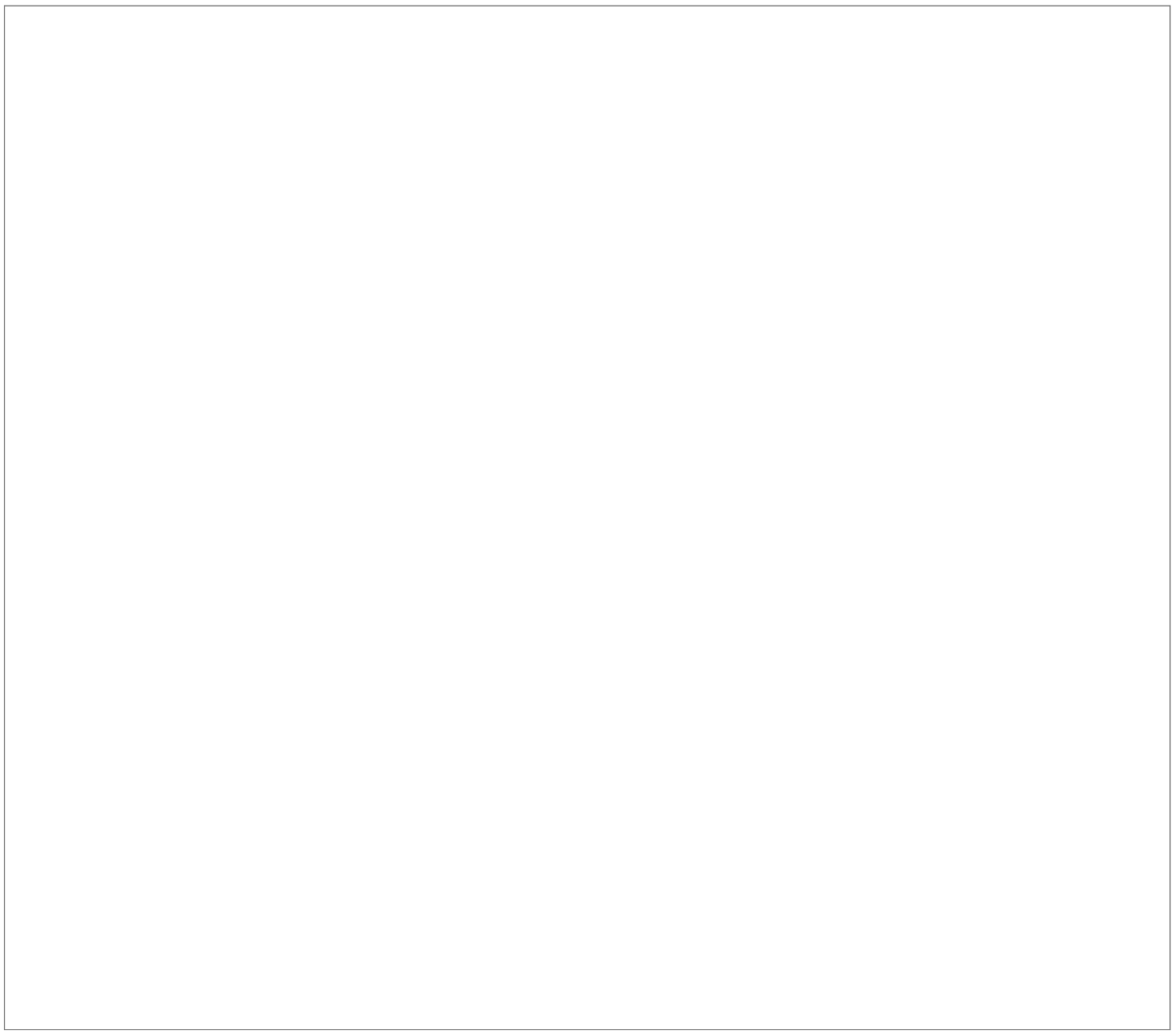
Post Privacy

Wenn im Bewerbungsgespräch ganz selbstverständlich Details aus dem Profil in einem sozialen Netzwerk besprochen werden, dann deutet das auf den Anfang eines grundlegend neuen Umgangs mit persönlichen Daten hin. Müssen wir uns auf das Ende der Privatheit einstellen – oder sollten wir ihr Ende gezielt anstreben? Führt die Metamorphose der Privatheit zu neuen sozialen Normen?

Unvermeidbare Datenoffenbarung

Angesichts der rechtlichen Bedeutung informationeller Selbstbestimmung und des Datenschutzes mutet eine Diskussion über das Ende der Privatheit befremdlich an. Wie weit staatlich regulierte Öffnung allerdings gehen kann, zeigt das Beispiel Schweden mit frei zugänglichen Steuerdaten und offenen Archiven über Vorstrafen. Werden solche Daten leicht zugänglich gemacht und intuitiv verständlich visualisiert, führen sie zu beträchtlichen Folgen nicht nur hinsichtlich Immobilienpreisen, Risikoklassen in Versicherungen und Kreditwürdigkeitsratings.
Die freiwillige und unfreiwillige Datenoffenbarung in sozialen Netzwerken, beim Online-Einkauf, bei der Nutzung des Smartphone, in Sensornetzwerken entzieht sich direkter rechtlicher Steuerung. Vernetzung, Bilderkennung und Analysemöglichkeiten für große, auch unstrukturierte Datenmengen eröffnen neue Möglichkeiten der Beobachtung jedes Einzelnen (siehe Digitale Unversehrtheit).

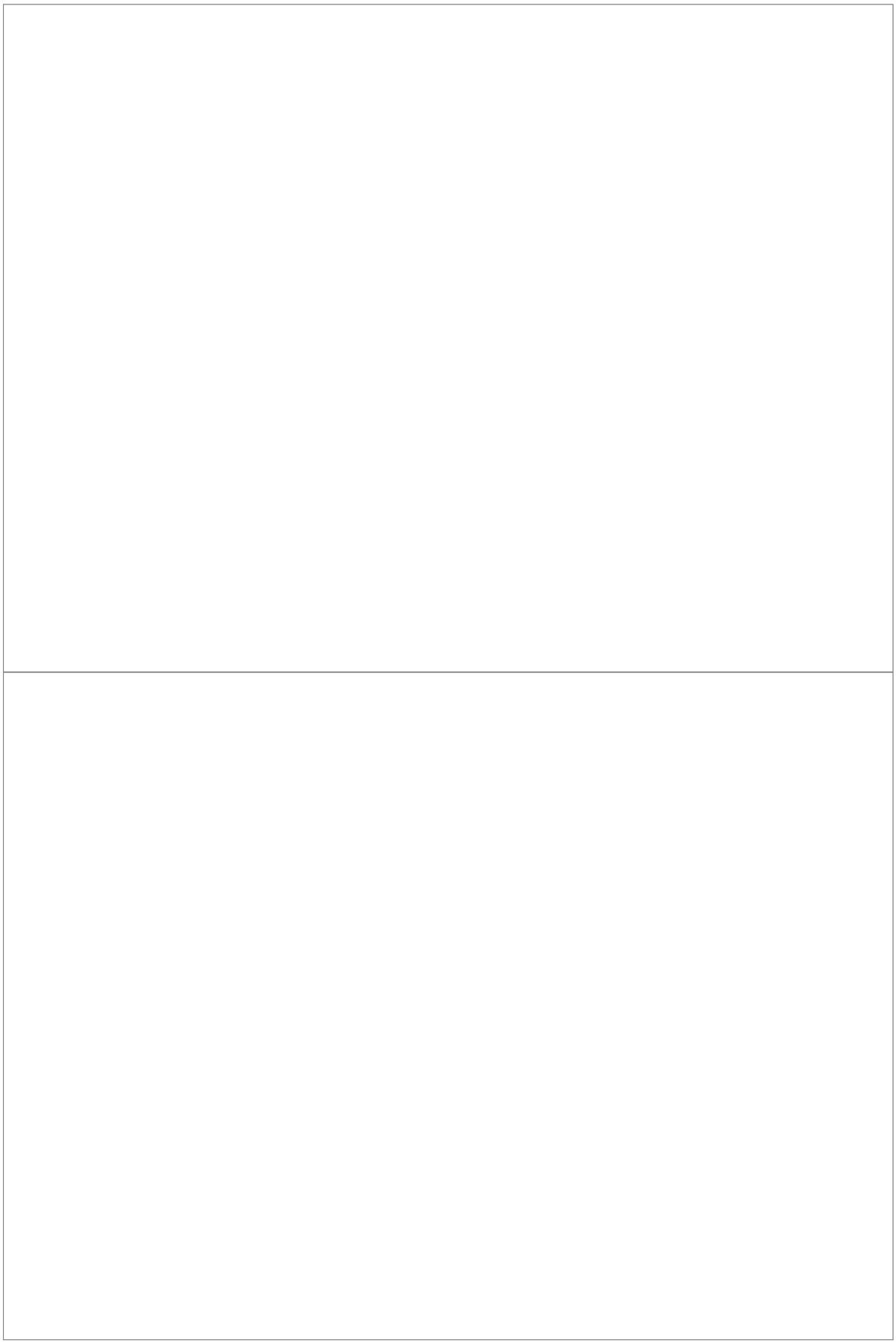
Begriffliche Verortung



Toleranz durch Offenheit

Es stellt sich die Frage, ob angesichts der für die Teilnahme am gesellschaftlichen Leben unvermeidlichen Datenoffenbarung und des einfachen Datenzugriffs die Aufrechterhaltung von Privatheit im heutigen Verständnis überhaupt noch möglich ist. Die empirische Frage lässt sich auch normativ wenden: Statt eines aussichtslosen Abwehrkampfes könnte die gezielte Offenlegung personenbezogener Daten (siehe Daten-Philanthrop) neue soziale Normen emergieren lassen. Die Erwartung neuer gesellschaftlicher Regeln erschließt sich nur mittelbar. Jenseits der psychologischen Funktion als Rückzugsgebiet erlaubt Privatheit das Verbergen und Vergessen diskreditierender Daten, was dem gesellschaftlichen Zusammenhalt förderlich sein kann.
Dieses Verbergen geht stets mit dem Risiko des Entdeckens und der Skandalisierung einher. Fraglich ist, ob bei prinzipieller Offenheit der Daten die alten Mechanismen der medientauglichen Aufdeckung von Einzelaspekten weiterhin Erfolg versprechen (siehe Massenmedien). In der normativen Wendung von Post Privacy wird aus dieser Überlegung ein kategorischer Imperativ: die Offenlegung alles Privaten führt zu einer neuen Dimension gesellschaftlicher Toleranz. Ob sich dieser gesellschaftliche Wandel angesichts einseitiger Verfügbarkeit von Daten und deren Analysemöglichkeiten als stabil erweist, bleibt eine offene, absehbar nur theoretisch zu erörternde Frage.

Themenkonjunkturen



Folgenabschätzung

Möglichkeiten

- Offenheit kann mit einer neuen Kultur der Toleranz einhergehen, was die Skandalisierungen von Lebensläufen erschwert
- Andersartigkeit von Minderheiten wird umfassend beobachtbar und dadurch trivialisiert
- Präferenzoffenbarungen erlauben eine Wirtschaft und Politik, bei der die Bedürfnisse des Menschen im Mittelpunkt stehen
- Der Grad der Offenbarung bleibt in Teilen selbstbestimmt

Wagnisse

- Privatheit wird zu einem Privileg für technisch Versierte und Wohlhabende
- Informationsasymmetrien zwischen Individuen und Gruppen schaffen umfassende Kontrollmöglichkeiten und Konformitätszwänge
- Offenheit wird für kriminelle Aktivitäten missbraucht
- Das Versicherungsprinzip fällt durch individuelle Risikoklassifizierung faktisch weg
- Erpressbarkeit, Mobbing und virtuelle Pranger werden auf eine neue Ebene gehoben
- Qualitative Einordnung und Quellenprüfung von Datensätzen wird nahezu unmöglich

Handlungsräume

Selbstbeschränkung

Post Privacy ist zunächst eine individuelle und gesellschaftliche Haltung. Dem öffentlichen Sektor kommt dabei eher die Funktion zu, Datenschutzgrundsätze zu bewahren, denn die Offenlegung personenbezogener Daten aktiv zu fördern.

Informationszugang

Unabhängig von Ausgestaltungsdetails wird das Datenangebot wachsen. Staatliche Aufgabe ist dabei die Gewährleistung eines offenen Zugangs für möglichst Viele, um Machtungleichgewichte aufgrund von Datenmonopolen zu vermeiden.

Datenhoheit

Für Bürgerinnen und Bürgern muss es möglich bleiben, die Hoheit über ihre Daten auszuüben. Hierzu muss der öffentliche Sektor technische Kompetenz vorhalten und bereitstellen. Leitfäden zur praktischen Anwendung von Kryptographie wären hier ein einfaches Beispiel.