

Privatheit und Öffentlichkeit im Jahr 2035 – drei Szenarien

Matthias Bärwolff

21. November 2011

Einleitung

Im Rahmen der vierten Collaboratory-Initiative wurden Szenarien für das Jahr 2035 erarbeitet, in denen mögliche Konstellationen „plausibel, logisch und spannend“ abgebildet werden. Dabei geht es weder um den Entwurf von Utopien, noch den Entwurf von Dystopien – ein gerade im hochbrisanten Themenfeld „Privatheit und Öffentlichkeit“ nicht immer einfaches Unterfangen.

Als weitgehend unstrittige gemeinsame Prämisse für alle folgenden Szenarien darf die schon jetzt offenkundliche Zunahme an Konfliktpotenzial durch Datenschutzprobleme im Allgemeinen und Datensicherheitsprobleme im Speziellen gelten. Es vergeht kaum ein Tag, an dem nicht Ausweitungen bei der Erhebung von privaten Daten durch Service-Anbieter im Internet vermeldet werden oder Sicherheitsprobleme bei der Verwahrung potenziell kritischer Daten bekannt werden. Wir sehen in dieser Realität einen fundamentalen Treiber für sowohl technischen Fortschritt (vor allem im Hinblick auf Geschäftsmodelle im „Social Web“) als auch gesellschaftlichen Diskurs zur Balance zwischen Privatheit und Öffentlichkeit, (vor allem dort, wo diese durch kommerzielle Akteure im Internet hergestellt wird).

Die Ergebnisse dieses Wechselspiels zwischen den beteiligten Stakeholdern – Endnutzer, Service-Anbieter, Regulierungsbehörden, soziale Normen – sind indessen nicht abzusehen; ebenso wenig wie die sozialen Normen zu Privatheit und Öffentlichkeit im Internet im Jahre 2035. Hier divergieren die drei von uns entwickelten Szenarien denn auch maßgeblich. Während in *Szenario 1* die Idee der Privat-„Sphäre“ fortbesteht und diese aktiv von Endnutzern gestaltet und gegenüber Dritten geschützt wird (und zudem soziale Normen dieses Paradigma stützen), sind es in *Szenario 2* große, staatlich regulierte und weitgehend vertikal integrierte Service-Anbieter, die Aspekte von Privatheit von Endnutzern schützen, die entsprechenden Aufgaben werden also hier von Endnutzern an zentrale Instanzen delegiert. In *Szenario 3* schließlich ist die Unterscheidung von Privatheit und Öffentlichkeit weitgehend aufgehoben, unterstützt durch sozial Normen sowie Rechtsgrundsätze zu Toleranz und Nichtdiskriminierung.

Szenario1: Individuelle Kontrolle

„Ja Papa, du hast ja recht.“ Julia hat jetzt eigentlich keine Lust mehr auf Diskussionen zur Wichtigkeit von informationeller Selbstbestimmung. „Macht geht immer ...“ sagt ihr Vater, und Julia beendet den Satz „... mit Verantwortung einher – schon klar.“ Morgen beginnt ihr halbjährlicher Online-Kurs zu „Endnutzeraspekten technischen Datenschutzes“, ohne den verliert ihre OIID – Open Internet ID – ihre Gültigkeit. Dabei hat sie doch eigentlich Wichtigeres zu tun in den nächsten Wochen.

Denn als IT and Privacy Consultant befasst sie sich von Berufs wegen täglich mit der Frage, wie Internet-Services so gestaltet werden können, dass möglichst keine personenbezogenen Daten überhaupt anfallen. Und dort wo sie anfallen, wie man den Nutzern größtmögliche Kontrolle darüber gibt, ohne dabei den Mehrwert des fraglichen Dienstes zu beeinträchtigen. Noch vor einiger Zeit hatte man geglaubt, Nutzer wären mit solcher Verantwortung überfordert; und alles über dreigliedrige Multiple-

Choice-Formulare hinaus wäre schlicht eine Zumutung. Was sich natürlich als Quatsch herausstellte. Nach den unzähligen Datenpannen in den 10er Jahren kam es nämlich zu einem erstaunlich zügigen kulturellen Wandel, praktisch im gesamten Internet-Ökosystem: gesellschaftliche Normen, rechtliche Rahmenbedingungen, technische Werkzeuge – kaum ein Bereich, der nicht explizit die Verantwortung und Kontrolle von Endnutzern über ihre eigenen Daten stützte. Sonst würde es das offene Internet wohl auch nicht mehr geben, überlegt Julia.

Unterdessen hat sie zuende gefrühstückt – ein Glas Sauerkrautsaft und zwei Brötchen mit Butter und Marmite. Gleich beginnt der Holo-Call – die holografische Telekonferenz – mit ihren Kollegen im Back Office. Gerade will sie noch kurz ihr Outfit prüfen, da bemerkt sie beim Blick auf ihr Konnex-Handy, dass der digitale Holo-Zugang zu ihrer Wohnung noch offen steht. „Da habe ich wohl gestern vergessen, mich aus der Konferenz auszuloggen“, denkt sie. Früher hätten sich sofort ein paar Skript-Kiddies in ihre Hologlobe eingeloggt, aber seit es schon im Kindergarten das Fach „Normen informationeller Selbstbestimmung“ gibt und Ende-zu-Ende-Verschlüsselung sämtlicher Datenströme in Internet zum globalen Standard geworden sind, passiert so etwas ja kaum noch. Und die Kollegen haben die Verbindung gestern sowieso von selbst geschlossen. „Gut, denn was ich morgens zum Frühstück esse, ist ja wohl auch nur meine Sache.“

Szenario 2: Delegierte Kontrolle

„Sich einfach mit ein paar Freunden treffen, in einem öffentlichen Cafe, das hat sich damals kaum noch jemand gewagt“, sagte Julias Mutter. Sie hatte sich von ihrer Tochter überreden lassen, mitzukommen zu deren allwöchentlichen Treffen mit Freundinnen. Und diese konnten es kaum glauben, wie schwer es noch vor nicht einmal 20 Jahren gewesen sein sollte, sich entspannt im öffentlichen Raum zu bewegen, ohne ständig Sorge haben zu müssen, am nächsten Tag indiskrete Fotos für alle Welt zugänglich im Internet zu finden. Und man konnte nichts dagegen machen. Außer eben zu

Hause bleiben, und auch dort war man ja kaum mehr sicher: Stromversorger, Internetanbieter, Lieferservices – alle konnten mit personenbezogenen Daten praktisch tun und lassen was sie wollten. Die Idee des Datenschutzes funktionierte einfach nicht mehr in einer weitgehend privatwirtschaftlich und auf Informationen basierenden Gesellschaft.

Julia schüttelt den Kopf. Wie gut, dass heute alle großen Anbieter im Social Web einem gemeinsamen Kodex folgen, nach dem Inhalte nicht ohne weiteres öffentlich gemacht werden können – schon gar nicht ohne das Einverständnis der betroffenen Personen. Damals hätte sie Fotos von ihrer angeheiterten Mutter inklusive Geo-Tags einfach so im Internet verbreiten können – kein Wunder, dass sich da niemand mehr auf die Straße getraut hat. Heute sind Inhalte mit einem digitalen Verfallsdatum ausgestattet, und die Anbieter tragen die Verantwortung dafür, sie nur für freigegebene Nutzergruppen abrufbar zu machen. Selbst speichern kann man solche Daten natürlich auch nicht mehr, das Konzept des „Personal Computers“ wurde durch immer raffiniertere Gadgets vollkommen überflüssig – heute benutzt praktisch jeder einen der „Private Spaces“ bei einem der verbliebenen drei internationalen Internet-Anbietern.

„Für uns ist aber auch nicht immer alles so einfach, wie es für dich erscheinen mag“, erwidert Julia ihrer Mutter. Gestern hat sie auf dem Nachhauseweg von der Firma ihren alten Studienkollegen Romeo getroffen. Und der ist bei „Amazebook“ angemeldet, sie hingegen bei „Akamoogole“. Kein Wunder, dass sie seit ihrem Webcommerce-Studium nichts mehr von ihm gehört hatte. Nicht mal telefonieren könnten die beiden miteinander, ohne eine eingehende staatliche Sicherheitsprüfung und Zahlung einer fünfstelligen Kautions für den Fall von IT-Sicherheitsproblemen bei der nötigen Zusammenschaltung ihrer beiden Accounts. „Früher hättet ihr euch einfach eine kostenlose E-Mail schreiben können oder Briefe per Post“, so Julias Mutter. Aber so etwas gibt es heute nicht mehr. „Wie sich doch das gesellschaftliche Grundverständnis von Kommunikation ändern kann, wenn Sicherheitsprobleme die Kosten nur genügend verschieben“, schließt Julia.

Als sie am nächsten Morgen aufwacht, hat sie die Diskussion des gestrigen Abends schon fast vergessen; eine wichtige Präsentation steht an diesem Vormittag an. Gestern Nachmittag hat sie an ihrem R2-D2-42-Computer auf dem Weg zu ihrer Mutter noch ein paar Änderungen eingearbeitet. Doch nun – oh weh! – sie muss den Computer im Taxi liegen lassen haben. Der erste Ärger ist jedoch schnell verflossen, schließlich liegen alle Daten sicher bei „Akamoogle“. Die Präsentation kann sie also auch von ihrem Konnex-Handy vorführen, und außerdem wollte sie sich sowieso bald das neue R3-D3-43 leasen.

Szenario 3: Soziale Kontrolle

Julias Holophone blinkt, ihre Tochter wurde gerade per Crowd-Lokalisierung im Schwimmbad eingecheckt. Und ihr Mann steht im Stau auf der A100. „Soweit sind wir also gekommen“, denkt sie: „Jeder weiß zwar von jedem, wo er steckt und was er gerade tut – aber weder die Hormone noch das Verkehrschaos haben wir in den Griff bekommen.“ Und das im Jahr 2035 Sie legt sich erschöpft auf die Couch. Wenn sowieso niemand pünktlich zum Abendessen kommt, dann kann sie endlich mal wieder in Ruhe Musik hören. Ihr Cred-Count – ihr Glaubwürdigkeitsindex – ist zwar, was ihre Musiksammlung angeht, gewohnt hoch; aber ihre Street Cred – ihr „Coolness-Faktor“ – sinkt schon seit Jahren. Höchste Zeit also, ihre MP3-Playlisten zu aktualisieren. Zwar gibt es dafür diverse Apps, aber es gibt schließlich auch immer neue Plausibilitätsprüfungsanbieter, da wird so etwas in den sozialen Netzen unbarmherzig und für alle Welt sichtbar abgestraft. Nur die unbedarfteren Zeitgenossen tappen in diese Falle; wie ihr Kollege neulich: Der wollte doch der ganzen Firma beweisen, wie jugendlich er geblieben ist. Erst wollte er gar keine Daten von sich preisgeben, und dann sowas. „Nein“, denkt sich Julia. Ihre Musiksammlung will sie schon ganz alleine auf Vordermann bringen.

Ihr Holophone blinkt erneut und summt im Takt der Musik. Julia überlegt kurz, ob sie rangehen soll. Sie weiß ja schon, dass ihre Tochter

heute erst spät nach Hause kommen will – die Sozialprofilanalyse ihres Konnex-Handys hat das schon vor einer Stunde angekündigt. „Kommunikation kann auch manchmal anstrengend sein, vor allem wenn es eigentlich nichts zu bereden gibt“, denkt sie. Mit ihren Playlists ist sie derweil ein gutes Stück vorangekommen; von Elvis sind nur noch zwei Titel dringelieben, das hatte sie noch nie geschafft. Die ersten Netzkontakte kommentieren ihre Auswahl neuer Musik – überwiegend wohlwollend. Julia ist ein bisschen stolz auf sich, und auch ihre Street Cred ist jetzt wieder im Sollbereich.

Sie ist gerade fertig mit ihrem privaten Exkurs ins Musische, als ihr Mann in die Tür kommt. Ganz altmodisch fragt er, wie ihr Tag war – altmodisch, denn sämtliche Daten ihres Tages liegen längst hochredundant archiviert und offen verfügbar im Internet. Wie auch die seinen und die aller anderen Bürger, zusammen mit den entsprechenden Identitätsmerkmalen, Gesundheitsindizes, Körperfunktionen, etc. Seitdem die Genomforschung in den 2020er Jahren den Begriff von Normalität zugunsten der Würdigung individueller Faktoren fast völlig aus dem gesellschaftlichen Diskurs verdrängt hat, sind entsprechende Bedenken rar geworden. „Wir sind alle nur Menschen“, sagt Julias Mann und lässt sich erschöpft in einen Sessel fallen. „Einem neuen Kollegen musste ich heute erklären, dass nicht nur seine politischen und sozialen Freiheiten außerhalb der Firma unter den absoluten Schutz der Verfassung fallen, sondern dass auch in der Firma Kritik und Verbesserungsvorschläge jenseits von Hierarchien ausdrücklich erwünscht sind. Schließlich kommt jede fundamentale Einsicht letztlich aus dem Geist des Einzelnen, selbst in einer Welt voller offener Daten und Crowd-Mechanismen.“ „Ich weiß“, antwortet Julia.