

- Sie versorgt dein Handy nicht nur mit Empfang, sie hilft auch, es zu orten.
- Ein Aprilscherz? Mitnichten! Hier wird nicht gescherzt, hier soll Verbrechen bekämpft werden. Deshalb ist sie seit dem 1. April 2012 in Österreich gesetzlich verankert.
- Ihr Name ist sozusagen Programm! Sie geben Auskunft darüber, wo sich ein Handy befindet.
- Diese Schnittstelle zur Datenübertragung via Funk trägt den Zahn nicht nur im Namen: In Sachen Datensicherheit zeigt sie nämlich schon mal gerne ihre Zähne und lässt allzu blauäugige SchnittstellennutzerInnen zwischendurch ganz schön blass aussehen.
- Wie sie im Detail umgesetzt wird, bleibt den einzelnen Mitgliedsstaaten überlassen. Wird sie allerdings nicht innerhalb der festgesetzten Frist in nationales Recht umgesetzt, so wie das im Fall der Vorratsdatenspeicherung in Österreich der Fall gewesen ist, so wird der säumige Staat verurteilt.
- Klingt nach aktuellem Stauservice! Tatsächlich allerdings geben sie Auskunft darüber, wann du mit wem wie lang mobil verbunden gewesen bist.
- Im Fall der Fälle schützt dich das Aus-dem-Verkehrs-Ziehen dieses kleinen Chips vor weiterem Schaden.
- Früher war dieses vor allem beim Computer Thema. Heute macht es jedes Smartphone zu einem kleinen PC. Und nachdem das tollste Handy nicht funktioniert, wenn es fehlerhaft ist, wird heute schon beim Handykauf darauf geachtet.
- Er tut weder dir noch deinem Handy gut! Beide werdet ihr davon krank.
- Mit seiner Eingabe entlockst du deinem Handy gewisse Informationen. Tippst du etwa *#06# ein, so wird die IMEI-Nummer deines Handys angezeigt, die dieses einzigartig und unverwechselbar macht.
- Ein niegelagertes Mobiltelefon verfügt über sie. Und zwar nur über sie. Werden sie wieder hergestellt, so wird alles andere gelöscht.





Alles klar?

V	O	R	A	T	S	D	A	T	E	N	S	T	A	N	D	O	R	T	D	A	T	E	N			
											S	I	M	K	A	R	T	E								
											B	L	U	E	T	O	O	T	H							
											B	E	T	R	I	E	B	S	S	Y	S	T	E	M		
											W	E	R	K	E	N	S	T	E	L	L	U	N	G	E	N
											V	E	R	K	E	H	R	A	T	E	N					
											T	A	S	T	E	N	C	O	D	E						
											E	U	R	I	C	H	E	R	U	N	G					
											E	F	U	N	K	Z	L	E	L	E						

- It provides the mobile phone not only with reception, but also helps to locate it.
- An April fool's joke? Not at all! This is no hoax, this is to fight crime. Therefore it has become law in Austria since 1 April 2012.
- Its name reflects its aim! It provides information about where a mobile phone is located.
- The name alone shows that this interface for data transmission via radio is by no means toothless: as regards data security it likes to show its teeth and makes naïve interface users sometimes look quite pale.
- The individual Member States are free to decide how to implement it in detail. However, if it is not implemented by a national law within the prescribed period, as it was the case in Austria with retention of data, the Member State in default is adjudicated.
- Sounds like an up-to-date service on traffic jams! Actually it provides information about when you were connected with whom via the mobile phone and for how long.
- If necessary, withdrawing this little chip from circulation protects you from further damage.
- In the past this was an issue especially with computers. Today it makes every smartphone a small PC. And as the smartest mobile phone does not work if it is defective, a special focus is laid thereon already when buying a mobile phone.
- It is no good, neither for you nor for your mobile phone! You both fall ill if you catch one.
- When typing it in you get certain information from your mobile phone. For example, if you type in *#06#, the IMEI number of your mobile phone is displayed which is unique and unmistakable.
- A brand-new mobile phone has them. And only them. If they are restored, everything else is deleted.



Be smart!

Die unten beschriebenen Fallbeispiele waren Teil des Einstiegs in das Thema „Datenschutz“. Jetzt, wo du mobiler Datenschutz-Profi bist, liegt es an dir: Verfasse Tipps, was man tun kann, um der jeweils beschriebenen Gefahr aus dem Weg zu gehen!



Paul S. & eine App mit unentdeckten



Als ich diese App entdeckt habe, war ich echt begeistert: „Beame mit nur einem Knopfdruck deine privaten Fotos in die Filmsets aktueller Blockbuster!“ Echt lässig! So lässig, dass sich auch alle meine Freunde über eine MMS freuen durften, in der sie an der Seite ihrer persönlichen Leinwandhelden zu bewundern waren. Echt cool! Haben übrigens auch alle meine Freunde gefunden!

Weniger cool war allerdings, dass wir kurze Zeit später mit SPAM-SMS überhäuft wurden. Und dann kam's auch schon in der Zeitung: Die Blockbuster-App konnte nämlich noch einiges mehr als auf Knopfdruck zu beamen. Ohne dass ich es bemerkt habe, hat sie auf meine persönlichen Kontakte und das Anrufverzeichnis zugegriffen. Und das Peinliche daran ist, dass ich dem App-Betreiber beim Installieren der App sogar die Erlaubnis dafür erteilt habe. Jetzt hoffe ich nur, dass nicht noch mehr Überraschungen auf mich warten. Würde mir grad noch fehlen, dass auch noch meine Handyfotos irgendwo im Web auftauchen ...

.....
.....
.....
.....

Sandra T. & verpasste Anrufe, die teuer zu stehen kommen ...



Meine letzte Handyabrechnung hat mich echt geschockt: Normalerweise zahle ich um die 12 Euro im Monat, und diesmal wurden alleine für Anrufe bei Mehrwertnummern mehr als 40 Euro verrechnet! Und das wo ich mir sicher war, keine kostenpflichtigen Nummern angerufen zu haben!

Nach dem ersten Schreck habe ich die Rechnungshotline meines Mobilfunkanbieters angerufen. Und als mich der nette Mann in der Leitung nach Anrufen unbekannter Nummern gefragt hat, war mir dann auch schon alles klar! Vor einiger Zeit hatte ich nämlich jede Menge verpasster Anrufe verschiedener Nummern. Und jedesmal wenn ich versucht habe zurückzurufen, bin ich in seltsamen Tonbandschleifen gelandet. So habe ich, ohne es zu merken, bei kostenpflichtigen Diensten angerufen und meine Telefonrechnung nach oben gekurbelt ...

.....
.....
.....



Isabella F. & die teure Gratis-App

„Drohende Gefahr durch Handy-Hacker“ – bis vor kurzem hab ich mir beim Lesen solcher Schlagzeilen gedacht, dass das ja wohl maßlos übertrieben ist. Seit letzter Woche sehe ich das allerdings ganz anders! Da bin ich nämlich selbst Opfer eines heimtückischen Angriffs durch Handy-Hacker geworden. Gemeinsam mit einer Gratis-App wurde mir – ebenfalls kostenlos, allerdings auch unerwünscht – ein Trojaner mitgeliefert. Und der hat dann, ohne dass ich es bemerkt habe, SMS an alle meine Kontakte verschickt. Erst als mich eine Freundin gefragt hat, warum ich eigentlich

dauernd leere SMS versende, habe ich gecheckt, dass da etwas nicht stimmen kann und meinen Mobilfunkanbieter angerufen. Da hat sich dann herausgestellt, dass von meinem Handy täglich um die 300 SMS versendet wurden ...

.....
.....
.....
.....



Tom K. & der *unheimliche* Shoppingtrip

Eigentlich hatte ich alles perfekt geplant! Am Montagmorgen war mir einfach ganz furchtbar übel, sodass ich nicht zur Schule gehen konnte. Und nachdem meine Eltern mich gebührend bemitleidet und sich in Richtung Arbeit begeben hatten, habe ich mich dann – unentdeckt von den Nachbarn – aus dem Haus geschlichen, bin zum Bahnhof gedüst und von dort direkt nach Graz weitergefahren: Shoppen statt Schulbank drücken! Während meines kleinen Ausflugs habe ich dann auch immer wieder meinen Status auf Facebook geändert. Mit meinem neuen Smartphone geht

das ja supereasy. Da hat dann eine Statusmeldung à la „Ich fühl mich soooo schlecht“ die nächste gejagt. Grundsätzlich genial! Dumm nur, dass ich vor einiger Zeit bei Facebook die Funktion aktiviert habe, dass bei jeder neuen Statusmeldung mein Aufenthaltsort automatisch ermittelt und im Profil angegeben wird. So konnten meine Eltern auf meinem Facebook-Profil meine Shoppingtour live mitverfolgen ...

.....
.....
.....
.....
.....



Florian E. & sein zweites Ich

Bis ich das Geld für mein neues Smartphone zusammengespart hatte, hat's eine gefühlte Ewigkeit gedauert. Die letzten Euro kamen dann noch aus der Onlineversteigerung meines alten Handys. Das Glück mit meinem neuen Smartphone hat allerdings nur bis letzten Freitag angehalten. Da hat mich nämlich einer aus der Parallelklasse mächtig dumm angemacht, von wegen: „Du treibst es ja ziemlich bunt, Loverboy2000“. Erst nach langem Hin und Her ist er dann endlich damit herausgerückt, was dieser dumme Spruch sollte. Auf einem bekannten Onlinedating-Portal gab's seit neuestem ein „Loverboy2000“-Profil. Und dieses Profil war mit privaten Fotos von mir gespickt. Der Käufer meines alten Handys hatte die Bilder offensichtlich entdeckt und es für besonders witzig und originell gehalten, damit „spaßhalber“ ein Profil auf dem Onlineportal anzulegen ...

.....
.....
.....
.....
.....



Zeynep K. & die Abofalle

Mein Klingelton hat mich schon lange genervt. Deswegen war ich auch Feuer und Flamme als ich meinen Lieblingssong als Klingelton gefunden habe. Ging auch ganz easy: Ich hab in der App einfach „Kaufen“ bestätigt, und schon stand mein neuer Klingelton zum Download bereit. So weit, so gut! Das böse Erwachen kam allerdings, als plötzlich das gesamte Guthaben auf meiner Wertkarte aufgebraucht war. Da hat sich dann herausgestellt, dass ich mit meinem Klick auf „Kaufen“ nicht nur den einen Klingelton, sondern gleich ein ganzes Klingeltonabo bestellt habe.

Ein teurer Spaß ...

.....
.....
.....
.....
.....



Smart & Safe

Be smart!



The following cases were part of the introduction into the topic of „data protection“. Now that you are a professional in mobile data protection, it is up to you: Create tips what to do to avoid the described risk!



An app with hidden possibilities

Paul S. was excited: thanks to a new app he was able to integrate his private photos into the film sets of recent blockbusters by pressing just one button! He had never ever sent as many multimedia messages like after he had installed this app. All his friends could admire themselves side by side with their movie heroes.

However, an unpleasant surprise was soon to come. What Paul S. did not know was that the app was far more powerful. And he himself had allowed the app and its operators to be so powerful. In order to be able to install the

app Paul S. had to give the app operators some authorisations, among other things access to his personal contacts and his call list. Data protectors now assume that such data was not only collected, but had also been passed on. And Paul S. now is afraid that he and his friends will in future receive loads of spam text messages and that his private photos may appear on any given websites.

.....
.....
.....
.....



Missed calls can be expensive ...

Sandra S. hardly could believe her eyes when she looked at her last mobile phone bill: she had been charged EUR 30 for calls to value-added service numbers which she just could not explain to herself! She calmed down and called the billing hotline of her mobile radio provider. Only when they asked for calls from unknown numbers she remembered the missed calls she had found on her mobile phone some time ago. She had always tried to call back but had only reached weird answering machine loops. Obviously she had called value-added services without noticing it! Her

contact at the hotline offered her to block her mobile phone for value-added service numbers.

.....
.....
.....
.....



Free app may be expensive ...

Last week Isabelle F., a student from Upper Austria, fell victim to a malicious attack of mobile phone hackers. Together with a free app she also received a free but unwanted Trojan which sent text messages to all her contacts without her noticing it. Only when her classmates asked her why she sent empty text messages she became suspicious. However, she found no empty text message in her outbox. Only when she called her mobile radio provider she learned that she had already exceeded the number of included free text messages and that approx. 300 text messages had been sent from her mobile phone per day.

.....
.....
.....
.....
.....



Hello, here I am!

Luke, Matthew and Jacob, three students from Deutschlandsberg, had planned everything very well. They started off on time in the morning and instead of going to school then went to the train station. They took the 8.05 train and went to Graz: they had planned to go shopping instead of attending school. They had even thought of changing their Facebook status several times during their little trip, always using similar phrases like: „I feel sooo sick“. Thanks to their new smartphones this was no problem at all. However, they had overlooked the fact that on their Facebook sites they had activated the function to automatically detect their location and state it on their profile together with every new status message. So their status messages read „I feel sooo sick“; however, Graz and not their home town was stated as their location on all three profiles. So the three truants got caught very quickly thanks to their digital lead.

.....
.....
.....
.....
.....



Alter ego

Florian E. was very happy with his new smartphone. He was so happy that he did not even think about his old mobile phone any more, which he had sold with profit. Until last Friday, when his colleague left the office and said: „Don't go too far, Loverboy85!“ Mr. E first looked puzzled; then, after he had asked several times, his colleague felt pity for him and explained what this „Loverboy“ thing was all about. He showed Mr. E the profile of a single man with the username „Loverboy85“ on a well-known online dating portal. And this profile was actually loaded with private photos of Mr. E. Mr. E. made some research and found out that the buyer of his old smartphone had found the photos and had created a profile on the online portal „just for fun“!

.....
.....
.....
.....
.....



Zeynep K. & the subscription

Zeynep K. always wanted a new ringtone. So she was thrilled when she found her favorite song for download as a ringtone in a new app. Was also quite easy: She only had to confirm „Buy“ and could download her new ringtone. The rude awakening came quickly, however. Because suddenly, the entire balance was used up on her prepaid card. With her click on “Buy” she not only ordered one ringtone, but a full subscription.

.....
.....
.....
.....
.....



Internet-Exhibitionisten „Spackeria“ „Privatsphäre ist sowas von Eighties“



Interview: Ole Reißmann; 10. März 2011.

www.spiegel.de/netzwelt/netzpolitik/0,1518,749831,00.html

Wir müssen uns von der Idee privater Daten im Internet verabschieden, sagt Julia Schramm. Im Interview mit SPIEGEL ONLINE erklärt die Mitgründerin der „datenschutzkritischen Spackeria“, warum der Datenschutz nicht mehr funktioniert und was es mit Post-Privacy auf sich hat.

SPIEGEL ONLINE: Der Datenschutz muss verbessert werden, darüber waren sich bisher Internetaktivisten und Politiker grundsätzlich einig. Alles Quatsch, sagt eine neue Gruppe, die Sie mitbegründet haben - private Daten lassen sich ohnehin nicht mehr schützen. Was will die „datenschutzkritische Spackeria“?

Schramm: Keine Macht den Datenschützern. Wir finden, dass die aktuelle Diskussion um den Schutz von Daten an der Realität vorbeigeht. Wir leben in einer vernetzten Welt, wo Privatsphäre durch das Internet nicht mehr möglich ist. Nun müssen wir sehen, wie wir damit umgehen.

SPIEGEL ONLINE: Der Grundsatz „Meine Daten gehören mir“ gilt nicht mehr?

Schramm: Das ist zwar ein schöner Anspruch, aber meine Daten können mir nicht mehr gehören. Wir haben längst die Kontrolle darüber verloren. Ob wir es nun gut finden oder nicht: Privatsphäre ist sowas von Eighties. (lacht)

SPIEGEL ONLINE: Warum holen wir uns dann nicht die Kontrolle zurück und stärken den Datenschutz?

Schramm: Wie denn? Der Aufwand, private Daten zu kontrollieren und zurückzuhalten, ist mittlerweile unverhältnismäßig hoch. Im Endeffekt können wir uns nicht dagegen wehren. Deswegen wollen wir eine Diskussion über Post-Privacy anstoßen, als Flucht nach vorne.

SPIEGEL ONLINE: Was meinen Sie mit Post-Privacy?

Schramm: Das ist erst mal eine Zustandsbeschreibung, wie der Begriff schon sagt, nach der Privatsphäre. Gleichzeitig ist es auch eine Utopie, die Idealvorstellung einer Gesellschaft, die Privatsphäre nicht mehr nötig hat, weil es keine Diskriminierung mehr gibt.

SPIEGEL ONLINE: Aber warum wird Privatsphäre dann überflüssig?

Schramm: Es mag dann zwar immer noch Platz für Privatsphäre geben, im Sinne der Trennung Hannah Arendts von öffentlichem und privatem Raum. Aber sie wird nicht mehr als Schutz notwendig. Viele Datenschützer argumentieren ja mit wirtschaftlichen und staatlichen Repressionen, die drohen, wenn die eigenen Daten nicht genug geschützt sind. Außerdem glaube ich, dass der Wunsch nach dem Schutz der Privatsphäre eine Reaktion auf eine unsichere und potentiell gefährliche Umgebung ist.

SPIEGEL ONLINE: Tatsächlich sammeln Unternehmen vielfach persönliche Daten und forschen uns aus. Das sollen wir uns gefallen lassen?

Schramm: Wir lehnen es jedenfalls ab, das mit Gewalt zu verhindern. Natürlich ist die Dominanz von einigen wenigen großen Internetfirmen wie Google oder Facebook bedenklich. Deswegen plädieren wir dafür, dass Menschen bewusst mit ihren Daten und dem Internet umgehen: Dort gibt es einfach keine Privatsphäre mehr. Aber das heißt noch lange nicht, dass Datenschutzgesetze aus der analogen Zeit das Internet einschränken müssen.

SPIEGEL ONLINE: Was ist denn das für eine Gewalt, von der sie sprechen?

Schramm: Ein Beispiel: Der Datenschützer in Niedersachsen hat dem Betreiber einer Website verboten, Google-Werbung auf seinen Seiten zu schalten. Die Begründung war, dass die IP-Adressen der Nutzer ungefragt an einen weiteren Server übertragen werden. Dabei ist das im Internet die Regel, sehr viele Seiten nutzen solche Dienste - und die Nutzer wissen das auch. Die Entscheidung dagegen ist eine Form von Staatsgewalt. [...]

SPIEGEL ONLINE: Ohne staatliche Regeln sind die Internetnutzer den Datenkraken ausgeliefert. Ist das nicht ein Widerspruch zum bewussten Umgang mit den persönlichen Daten?

Schramm: Im Internet ist es eben vorbei mit der Privatsphäre, darüber sollte man sich klar sein. Schon der Begriff Datenschutz gaukelt eine falsche Sicherheit vor, die es praktisch nicht mehr gibt. Die einzige Alternative ist, anonym zu surfen.

SPIEGEL ONLINE: Sie geben viel von sich im Internet preis, unter anderem auf Twitter und in ihrem Blog. Gibt es da Grenzen?

Schramm: Ich habe die Erfahrung gemacht, dass ich im Gegenzug auch viel zurückbekomme, neue Freundschaften, Anregungen, Unterstützung. Einige Freunde haben mir gesagt, dass ich nicht über sie schreiben soll, das respektiere ich natürlich. Und ich muss mit den Konsequenzen rechnen: Wenn ich mich irgendwo bewerbe, kann mein Chef mit Google sofort herausfinden, dass ich für die Piratenpartei bei einer Wahl angetreten bin. [...]

SPIEGEL ONLINE: Wie also soll der neue Datenschutz aussehen?

Schramm: Genau darüber wollen wir jetzt diskutieren, eine Antwort haben wir noch nicht. Nur so viel ist klar: Wir müssen den Begriff neu definieren. Was sind überhaupt schützenswerte Daten - und wie kann man sie schützen? Mit einem digitalen Radiergummi doch ganz sicher nicht.



Analysefragen

Wie definiert Schramm den Begriff „Post-Privacy“?

Schramm kritisiert Datenschützer. Welche Argumente führt sie dabei an?

Worauf führt Schramm den Wunsch vieler Menschen nach mehr Schutz der Privatsphäre zurück?

Was hältst du von Schramms Ansichten? In welchen Punkten bist du ihrer Meinung, in welchen Punkten widersprichst du ihr?



Adieu, Privatsphäre - Goodbye, verstaubter Datenschutz

Christian Heller, Vertreter der „Post Privacy“-These, erklärt, wieso Privatsphäre ausgedient hat

Interview: Eva Zelechowski, 31. Jänner 2012.

<http://derstandard.at/1325485653364/Post-Privacy-Adieu-Privatsphaere---Goodbye-verstaubter-Datenschutz>

Haben „Datenschutz“ und „Privatsphäre“ ausgedient? Während die einen auf Informationssicherheit pochen, formiert sich anderswo eine Gegenentwicklung, die sagt, dass Datenschutz nicht funktioniert - zumindest nicht in seiner bestehenden Form. Christian Heller hat als einer ihrer Vertreter das erste Buch zum Thema, „Post Privacy - Prima leben ohne Privatsphäre“, geschrieben. Darin erklärt er, wieso Datenschutz den gestellten Sicherheitsanspruch nicht erfüllt und wieso es sich ohne Privatsphäre besser lebt. [...]

derStandard.at: Sind Sie selbst bereit, komplett auf Ihre Privatsphäre zu verzichten?

Christian Heller: Ich stelle ja sehr viel von mir ins Internet, zum Beispiel über mein Wiki, wo ich meinen Tagesablauf veröffentliche. Ähnlich wie viele Nutzer von Facebook und Twitter, die dort ihr Leben „hineinverdaten“. Es ist eher ein Experiment, und ich gehe sehr vorsichtig mit der Privatsphäre anderer um. Dritte werden von mir als „X“ bezeichnet. Den Kontrollverlust möchte ich schließlich anderen nicht aufzwingen.

derStandard.at: Welche Konsequenzen haben sich aus diesem Experiment ergeben?

Heller: Außer, dass sich dadurch Scherzanrufe bei mir gehäuft haben, habe ich bisher eigentlich keine konkreten Nachteile beobachten können.

derStandard.at: Sie haben vor kurzem Ihr Buch „Post Privacy - Prima leben ohne Privatsphäre“ veröffentlicht. Welche Meinung vertreten Sie darin konkret?

Heller: Informationelle Privatsphäre, also die Kontrolle darüber, was die Welt über mein Leben wissen kann, ist immer schwerer aufrechtzuerhalten. Vor allem in Anbetracht von Digitalisierung und globaler Vernetzung. Anstatt diese Entwicklungen zu bekämpfen, sollten wir schauen, wie wir damit klarkommen und das Beste daraus machen.

derStandard.at: Wieso ist das immer schwieriger?

Heller: Wir sind umgeben von einer wachsenden Menge an Aufzeichnungsmaschinen, die Informationen sammeln, miteinander verknüpfen und auswerten. Wir selbst sind es außerdem, die immer mehr Informationen in diese Maschinerie hineinstopfen - beispielsweise die 800 Millionen User bei Facebook. Auch durch andere wird immer mehr unseres Umfelds und unserer Umrisse darin abgebildet, sodass wir gar nicht aktiv daran teilhaben müssen - irgendwann haben wir wenig Möglichkeit, unsere Privatsphäre aufrechtzuerhalten. Gleichzeitig wachsen die technologischen Möglichkeiten mit leistungsfähigeren Computern und billigeren Speichern, um aus Informationen immer mehr Wissen zu hebeln und auch mehr Informationen zu sammeln.

derStandard.at: Wir sollten also nicht versuchen uns zu wehren? Wir scheitern mit dem Versuch, unsere Privatsphäre zu wahren?

Heller: Wahrscheinlich kann man das hie und da hinausögern, indem man sich dagegen wehrt. Letztendlich denke ich, dass unsere Kraft besser investiert ist, wenn wir mit den Bedingungen aus Offenheit und Transparenz umzugehen lernen anstelle nach Mechanismen zur Geheimhaltung zu suchen.

derStandard.at: Wo sehen Sie die größten Vorteile der Post-Privacy-These? Und gilt sie für alle gleich?

Heller: Vor allem nimmt die Kommunikation und gesamt-gesellschaftliche Transparenz zu, die Gesellschaft wird dank Post-Privacy intelligenter und solidarischer. Gemeinsame Interessen oder Unterschiede werden klarer hervorgehoben, was uns auch mehr Wissen darüber verschafft, wie wir unsere Probleme angehen können. Gleichzeitig werden Machtansammlungen durchsichtiger und damit demokratisch kontrollierbarer. Hier stellt sich die Frage, ob Post Privacy für alle gleich gilt und ob sich alle allen gegenüber gleichermaßen „nackt machen“ müssen. Oder ob es Institutionen wie Geheimdienste gibt, die sich erfolgreich dagegen wehren.

derStandard.at: Wie wäre in dem Fall Ihr Lösungsansatz?



Heller: Wenn es schon einen Überwachungsapparat gibt und wenn wir unsere Privatsphäre gegenüber Körpern wie Facebook oder Geheimdiensten aufgeben müssen, muss gewährleistet sein, dass dies symmetrisch geschieht. Dann auch bitte alle Daten von allen und Bekämpfung von Informationsmonopolen, wo versucht wird, das angesammelte Wissen nur wenigen Mächtigen zur Verfügung zu stellen.

derStandard.at: Sie erwähnten vorhin eine bessere Transparenz über gemeinsame Interessen. Können Sie ein konkretes Beispiel nennen?

Heller: Ein klassisches Beispiel sind Subkulturen, die tabuisiert sind, wie zum Beispiel sexuelle Subkulturen. Die lassen sich im Internet sehr leicht finden, da sehr viele User nicht zögern, sich mit ihrem Fetisch darzustellen. Teilweise geschieht das mit Pseudonymen, es ist also nicht die totale Post Privacy, aber man findet den Mechanismus, dass man traditionelle Tabu-Themen konkret im Internet artikuliert und als Person auch ansprechbar bleibt. Das ist meines Erachtens ein ähnlicher Effekt wie in der Homosexuellen-Bewegung, die der Gesellschaft mehr Respekt eingefordert hat und sich durch die Solidarität sehr viel stärker als Gemeinschaft fühlt.

Ein anderes Beispiel sind Menschen, die aus bestimmten sozialen Bedingungen wie Hartz IV Empfänger oder - sagen wir - Freiberufler ihre Lebensumstände im Netz dokumentieren und gemeinsame Strategien im Umgang mit Behörden oder adäquate Honorar-Verrechnungen austauschen.

derStandard.at: Wir haben also Ihrer Meinung nach Vorteile durch den zunehmend wegbröckelnden Datenschutz. Finden Sie auch, dass sich für die Gesellschaft auch Nachteile durch den Datenschutz ergeben?

Heller: Zum Teil. Erstens glaube ich auch, dass Post Privacy auch Nachteile mit sich bringt, weil dadurch Sicherheiten - auf die wir angewiesen sind - infrage gestellt werden. Datenschutz hat auf jeden Fall positive Aspekte, ist aber in der jetzigen Form meines Erachtens sehr zahnlos und machtlos. Nämlich dort, wo tatsächlich Daten geschützt werden müssen. Sprich, dort wo's weh tut, ist Datenschutz nicht das große Schutzinstrument für den Einzelnen.

Andererseits ist Datenschutz deshalb erträglich, weil er so wenig fasst.

Es gibt ein erhebliches Vollzugsdefizit. Würden aber tatsächlich die deutschen Datenschutzgesetze durchgesetzt, würde man das Internet zu einem zentralistisch regulierten, stark zensierten Gebilde umwuchten müssen. Das ist aber kaum erstrebenswert. [...]

derStandard.at: Sie schreiben in Ihrem Buch, dass es eine Art Selbstkontrolle ist, seine Agenden im Netz öffentlich zugänglich zu machen. Entmündigt man sich dadurch nicht auch etwas?

Heller: Das ist ein simpler Selbstdisziplinierungstrick. Wenn man ein Mensch ist, der schwer Termine einhält, hilft es, diese anderen mitzuteilen, um den sozialen Druck zu erhöhen. Letztendlich entscheide ich aber immer noch selbst und man könnte es eher ein Selbstkontrollinstrument nennen.

derStandard.at: Bekommt die These, die Sie vertreten, viel Zustimmung?

Heller: Es sind zwar nicht alle meiner Meinung, aber grundsätzlich räumen viele ein, dass es großen Diskussionsbedarf gibt. Viele stimmen zu, dass wir mit einem bestimmten Maß an Datenschutzverlust klarkommen müssen. Selten sind meine Gesprächspartner der Ansicht, dass Datenschutz, wie er jetzt - zumindest in Deutschland - ins Gesetz gegossen ist, gut ist. Ein Großteil stimmt einer Reformierung zu. Die Dimension der Radikalität ist eher ein Streitpunkt.

derStandard.at: Es sind also immer mehr Menschen, mit denen Sie sprechen, der Meinung, dass Privatsphäre in der Form, wie sie bisher oder vor den sozialen Netzwerken bestand, ausgedient hat?

Heller: Zumindest habe ich schon lange nicht mehr mit jemandem gesprochen, der die Position „Wir müssen alles tun, um die Privatsphäre zu schützen“ vertreten hat. Da bin ich mit meinem Buch nicht alleine, es hat sich inzwischen eine Bewegung formiert. Jene, die Facebook und Co. nicht nutzen, können die Geschwindigkeit dämpfen, mit der man ins kalte Wasser der Post Privacy stürzt. Gerade Facebook und seine Gewalt ist nicht zu unterschätzen, mit der sie versuchen die Entwicklung zu ihren eigenen Gunsten voranzutreiben. Während man den Eindruck heuchelt, man würde bloß einen Trend abbilden, ist man treibende Kraft hinter der Entwicklung.

derStandard.at: Ohne Facebook gewinne ich also ein bisschen Zeit vor dem Kontrollverlust meiner persönlichen Daten?

Heller: Ja, einige Jahre bekommt man dadurch schon. Im Zweifelsfall gerät man durch die Freunde in die Maschinerie hinein. Das große Problem von Facebook ist das Ungleichgewicht der Informationen - Facebook weiß alles über uns, wir wissen nichts über Facebook. Diese Daten müssen symmetrisch sein.



Analysefragen

Welche Meinung vertritt Heller in Sachen „Post Privacy“?

.....
.....

Heller führt einige Vor- und Nachteile des zunehmenden Verlustes des Datenschutzes an. Wie lauten diese?

.....
.....

Heller spricht von mehr Transparenz in unserer Gesellschaft durch den Verlust von Datenschutz, stellt allerdings in diesem Zusammenhang auch eine konkrete Forderung. Wie lautet diese?

.....
.....

Wie nimmt Heller die Einstellung seiner Umwelt zu Post Privacy wahr? Welche Meinung/en sieht er hier hauptsächlich vertreten?

.....
.....

Welche Maßnahme/n nennt Heller, um den Verlust der Privatsphäre hinauszuzögern?

.....
.....

Heller kritisiert Facebook. Welche Kritikpunkte führt er an?

.....
.....

Was hältst du von Hellers Ansichten? In welchen Punkten bist du seiner Meinung, in welchen Punkten widersprichst du ihm?

.....
.....

.....

Vocabulary

			
abbreviation	Abkürzung	misuse	Missbrauch
access	Zugriff	mobile phone	Handy
accounting purpose	Rechnungszweck	mobile radio provider	Mobilfunkbetreiber
additional service	Zusatzservice	mobile radio station	Mobilfunkstation
approval of a court	richterliche Genehmigung	operating system	Betriebssystem
area	Bereich	personal data	persönliche Daten
as a rule	aus Prinzip	phone memory	Telefonspeicher
backup	Sicherung	point-to-point radio	Richtfunk
balance	Gutschrift	public prosecutor	Staatsanwalt
bargain	Schnäppchen	radio cell	Funkzelle
battery	Akku	radio switching station	Funkvermittlungsstation
call	Anruf	radio wave	Funkwelle
call forwarding	Rufweiterleitung	reception	Empfang
call redirection	Rufumleitung	requirement	Anliegen
caller	Anrufer	retention of data	Vorratsdatenspeicherung
commencement	Beginn	satellite system	Satellitensystem
connection	Verbindung	secrecy	Geheimhaltung
consent	Zustimmung	security lapse	Sicherheitslücke
content data	Inhaltsdaten	security risk	Sicherheitsrisiko
contract	Vertrag	sensitive data	sensible Daten
corresponding receiver	Empfangsstation	signal transit time	Signallaufzeit
data deserving special protection	besonders schutzwürdige Daten	significance	Stellenwert, Bedeutung
data protection authority	Datenschutzbehörde	sky-rocketing	rasant ansteigend
data trace	Datenspur	space	Weltall
data traffic	Datenverkehr	storage place	Speicherplatz
data volume	Datenvolumen	store card	Kundenkarte
duration	Dauer	subscriber	Teilnehmer
emergency service	Notfalldienst	surveillance system	Aufsichtsstelle
EU Directive	EU Richtlinie	sweepstake	Gewinnspiel
exchange of data	Datenaustausch	technological impact assessment	Technikfolgenabschätzung
factory reset	Werkseinstellung	theft	Diebstahl
free home	frei Haus	to allocate	zuweisen, vergeben
frequency	Häufigkeit	to apply	zutreffen
intersection	Schnittpunkt	to ascertain	ermitteln
legal protection	Rechtsschutz	to avoid	vermeiden
master data	Stammdaten	to be aware of	sich einer Sache bewusst sein
message	Nachricht	to bear	in sich bergen

	
to block	sperren
to charge	verrechnen
to contribute to something	zu etwas beitragen
to create	produzieren
to delete	löschen
to determine	feststellen, bestimmen
to enter	eingeben, eintreten
to estimate	abschätzen, ermessen
to forward	weiterleiten, versenden
to fulfil	erfüllen
to grant	gewähren
to identify	identifizieren
to install	installieren
to issue	ausstellen
to locate	lokalisieren
to maintain	erhalten, wahren
to monitor	abhören, überwachen
to orbit	umkreisen
to prosecute	gerichtlich verfolgen
to provide	versorgen
to record	aufnehmen
to remain	(ver-)bleiben, bestehen bleiben
to remove	entfernen
to request	fordern
to require	anfordern, verlangen
to restore	wiederherstellen
to retrieve	abrufen
to state	angeben, erklären, behaupten
to stipulate	festlegen
to store	speichern
to take into account	berücksichtigen
to transmit	übertragen, senden
to turn on	einschalten
to weigh something	etwas abwägen
traffic data	Verkehrsdaten
Trojan	Trojaner
user manual	Gebrauchsanweisung
weather forecast	Wettervorhersage