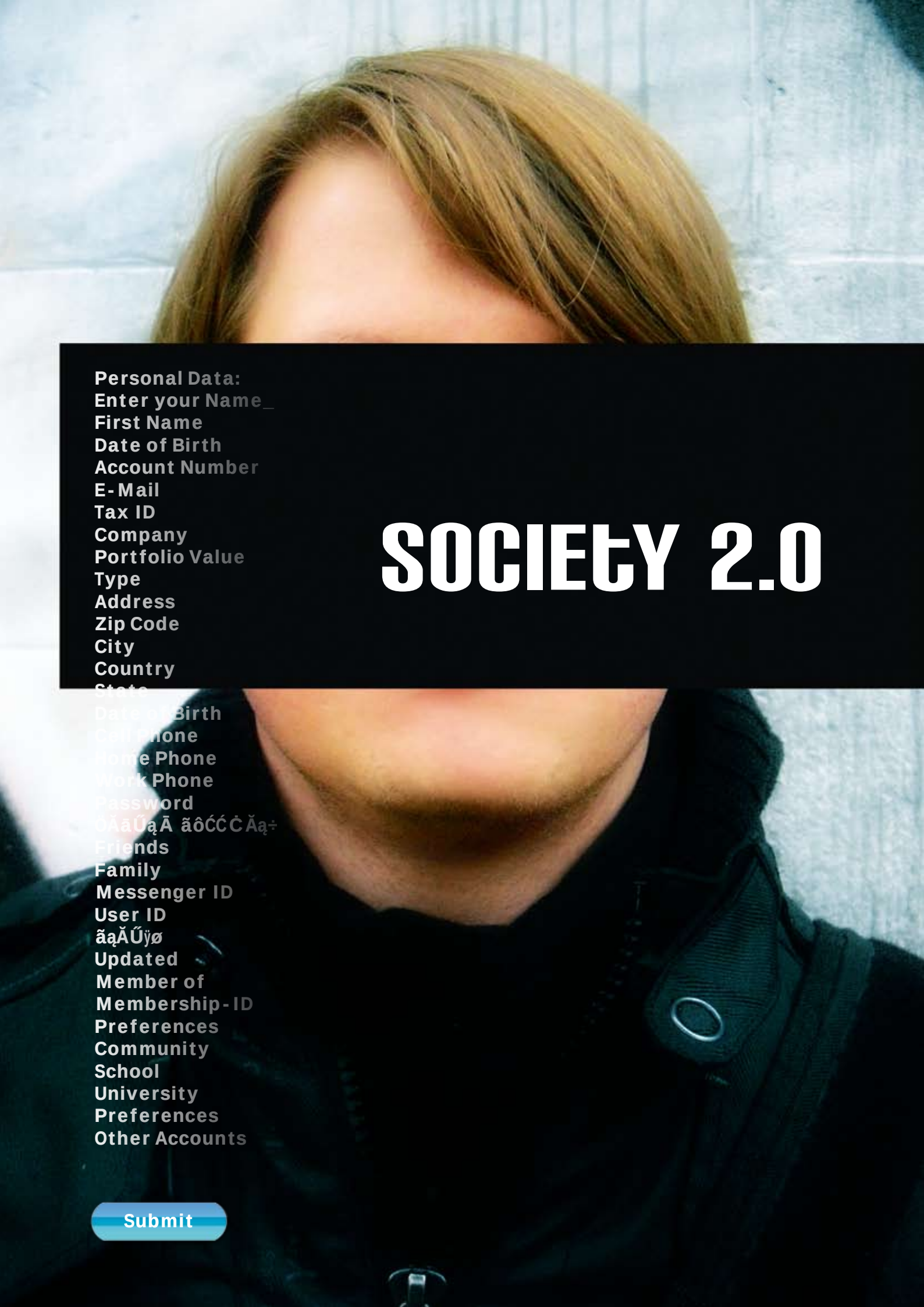

SOCIETY 2.0
Personal Data:
Enter your Name_
First Name
Date of Birth
Account Number
E-Mail
Tax ID
Company
Portfolio Value
Type
Address
Zip Code
City
Country
Date of Birth
Cell Phone
Home Phone
Work Phone
Password
Friends
Family
Messenger ID
User ID
Updated
Member of
Membership-ID
Preferences
Community
School
University
Preferences
Other Accounts
Submit

Krieg bedeutet Frieden.
Freiheit ist Sklaverei.
Unwissenheit ist Stärke.

George Orwell, 1984.

2008

FH Potsdam

Interfacedesign

Bachelor

SOCIETY 2.0

Melanie Skowronek

INHALT

MOTIVATION

Warum mache ich das?

Im Interfacedesign-Studium begegnete ich verschiedensten Technologien und kleinen Erfindungen, die das tägliche Leben leichter machen und unterstützen sollen.
Der Umgang mit Chips, Platinen, Mini-Kameras, verschiedenen Verschlüsselungsmethoden u.ä. ist dabei für die meisten meiner Mitstudenten ganz selbstverständlich. All diese Dinge sind Mittel zum Zweck auf dem Weg zu neuem Design.
Mit der Zeit merkte ich, dass bei all der Begeisterung für neueste Technik eine Sache auf der Strecke blieb:
Die kritische Auseinandersetzung mit einigen der verbauten Einzelteile oder bearbeiteten Inhalte.
Ich selbst arbeitete in einem Kurs an einem Prototypen für die elektronische Gesundheitskarte mit. Im Designprozess konzentrierten wir uns vor allem darauf, den Anforderungen und Funktionen der Karte gerecht zu werden.
Heute steht der Entwurf für die Karte, mit einigen Features, die auch wir damals ersannen. Allerdings entwickelt sich gerade eine Diskussion um das Potenzial der gespeicherten Gesundheitsdaten und die Angst vor deren Missbrauch durch Dritte.
So weit haben wir mit unserem Entwurf gar nicht gedacht, weil uns die Hintergründe fehlten. Ich für meinen Teil hätte mich im Nachhinein gern näher mit der diskutierten Problematik beschäftigt, um auch dafür einen Lösungsansatz zu finden. Unsere Arbeit im Kurs endete jedoch an der Stelle, wo alle Features gefunden, beschrieben und untergebracht waren.
Es war interessant, sich mit einer komplexen Thematik zu beschäftigen und ein Interface dafür zu entwickeln, die Idee der Karte ist auch grundsätzlich gut. Es fehlte dennoch an einiger Stelle die Diskussion oder Abschätzung des Gefahrenpotenzials dieser Weiterentwicklung des Mediums, das so viele persönliche Daten trägt und für jeden zur Pflicht werden soll.
Meine Arbeit ist genau diese Beschäftigung mit der Frage: Was ist, wenn die gute Erfindung für einen schlechten Zweck missbraucht wird? Kann man Technologie, die eigentlich dafür gebaut ist, Arbeitsprozesse, Forschung oder einfach Lebensqualität für den Menschen zu verbessern, auch gegen ihn einsetzen? Ich will herausfinden, wie es sich anfühlt, wenn viele einzeln harmlos wirkende Methoden und Technologien vernetzt in einem Szenario zusammenlaufen, das plötzlich jeden bedrohen kann.
Mein Schwerpunkt wird dabei immer die Kritik an den vorgestellen Dingen und Umständen sein. Ich möchte dazu anregen, dass wir uns auch mit den (Missbrauchs-) Risiken beschäftigen, die unsere Erfindungen in sich bergen. Dadurch ergibt sich die Chance ihre Möglichkeiten voll auszuschöpfen und sie noch effizienter zu machen.
Jeder Designer sollte auch ein Gefühl für die Konsequenzen entwickeln, die seine Gestaltung haben kann. Es ist immer von Vorteil, auch auf Kritiker zu hören und auf Unsicherheiten seitens des Benutzers vorbereitet zu sein und eingehen zu können.
Diese Sensibilisierung ist ein wichtiger Schritt zur klugen Weiterentwicklung vorhandener Technologien und wird in Zukunft wegweisend für neue Anwendungen sein.

Ziel der Arbeit

Die erste Überlegung für diese Arbeit war: Für wen oder welchen Fall kann die Entwicklung effizienterer Technik in Zukunft interessant sein und vor allem, unter welchen Umständen könnte sich der positive Zweck, für den sie erfunden wurde, ins Gegenteil umkehren?
Überwachungsstaat 2.0 ist das Schlagwort für mein Vorhaben. Allerdings geht es nicht darum, Stimmung gegen Sicherheitstechnik oder staatliche Entscheidungen zu machen. Vielmehr soll ein Gefühl dafür vermittelt werden, was es heißt, sich zu sehr auf ein bestehendes System und seine „Macher“ zu verlassen und all seinen Maßnahmen unkritisch gegenüber zu stehen. Ich möchte zur Auseinandersetzung mit dem Thema anregen. Meine Arbeit soll jedoch nicht nur bestehende Maßnahmen dokumentieren und Möglichkeiten finden, sich davor zu schützen, sondern vor allem eine zukünftige Version des Überwachunsstaates erlebbar machen.

EINLEITUNG

Wo wird das alles hinführen?

Wenn man sich und andere fragt: „Wann hat das eigentlich alles angefangen?“, bekommt man meist die Antwort: Mit dem 11. September. Dieses Datum ist wie der Startschuss für eine Gesellschaft, die sich zunehmend Hollywood-filmreif in Szene setzt. We're the stars of CCTV [1] ist ihr Motto, Angst ihr Motor.

Es scheint, als sei an diesem Tag etwas ganz Grundsätzliches verloren gegangen. Vielleicht das Recht auf Freiheit, vielleicht aber auch der Glaube an das Gute im Menschen und die Hoffnung darauf, das wir mit friedlichen Mitteln unsere Konflikte lösen? Fest steht, dass seitdem etwas anders ist, überall auf der Welt und vor allem da, wo es den Menschen eigentlich gut geht, wo das Leben in geordneten Bahnen verläuft, Machtverhältnisse anerkannt sind, der Institution Staat weitestgehend Vertrauen geschenkt wird... Da, wo genug Geld, Know-How und Kräfte vorhanden sein sollten, um den Menschen das Gefühl von Sicherheit zu vermitteln, wächst die Angst stetig. Aber was genau ist eigentlich seit jenem grausamen Anschlag mit uns geschehen? Was hat sich genau verändert? Wo stehen wir heute mit unseren neuen Erkenntnissen, Technologien und Werten?

Das Leben ist weitergegangen, mit der Gewissheit, dass niemand unantastbar ist, auch nicht der Größte und Stärkste. In diesem Bewusstsein hat die Welt aufgerüstet, will sich auf alles einstellen und vorbereitet sein. Das Geschäft mit der gefühlten Sicherheit boomt. Unzählige neue Technologien brechen die Privatsphäre Einzelner auf. Für jeden Zweck gibt es eine Erfindung. Wir können alles herausfinden, über jeden. Aber reicht es, pauschal einfach Daten zu erfassen, zu kontrollieren oder zu scannen, um dann anhand von Auffälligkeiten einen Zugriff zu starten? Verhindert man so Verbrechen oder gar Anschläge? Hilft man der Gesellschaft, einige ihrer Schwierigkeiten in den Griff zu bekommen, wenn man nur genügend Überwachung schafft? Selbst die Einstellung zum Gebilde Staat hat sich gewandelt: Die Menschen wollen Sicherheit, wollen sich beschützt fühlen. Der Staat soll das irgendwie leisten. Dafür nehmen zunehmend viele in Kauf, dass verschiedene Organisationen und Einrichtungen immer mehr in ihr Leben eindringen, Daten erfassen, sammeln und speichern. Menschen gehen nicht mehr einfach nur von A nach B, sie generieren Bewegungsprofile. Fast beiläufig werden Gesetze erlassen, die es Staatsdienern leichter machen, mehr über uns zu erfahren, alles zum Schutz der Allgemeinheit. Wie geht man im täglichen Leben damit um? Ab wann verhält man sich verdächtig? Ist Überwachung wirklich so harmlos, dass wir sie einfach integrieren, fast ignorieren können? Wer nichts zu verbergen hat, kann eben so gut alles preisgeben. Sogar seine Freiheit.

Ist es für uns wirklich so unbedenklich, dass jeder der über die nötige Technik verfügt, Einblick in das Leben jeder beliebigen Person bekommen kann? Dass er Vorlieben, Neigungen, Ängste und Nöte, Freunde, Gewohnheiten, sogar Äußerungen und Gedanken einfach mitschneidet, interpretiert und vielleicht gegen diese Personen auslegen kann – einfach, weil er die Möglichkeit dazu hat? Das Ausmaß der staatlichen Überwachung ist für uns nicht begreifbar. Wir bekommen es erst dann zu spüren, wenn wir uns auffällig verhalten, nicht wie gewünscht funktionieren, oder vielleicht auch, weil ein System versagt hat.

Erst dann, wenn wir selbst anfangen müssen, das Gegenteil von dem zu beweisen, was uns zur Last gelegt wird. Aber dann ist es vielleicht schon zu spät. Die Vergangenheit hat viele Probleme im Umgang mit automatisch ausgewerteten Daten gezeigt. Oft war es ein falsches Wort am Telefon, eine Hoax-Mail, ein Urlaub in einem verdächtigen Land oder eben auch die „falsche“ Nationalität, die Behörden zum Handeln veranlasste und so normale Menschen zu Verdächtigen werden ließ. Voreilige Schlüsse brachten Unschuldige ins Gefängnis oder sogar bis nach Guantanamo*. Die Kontrolle wird zunehmend zum Zwang. Die Angst zu Paranoia. Der Staat mutiert zu unserem Vormund. Man schürt die Angst vor erneuten, noch grausameren Anschlägen, um immer neue Überwachungsmaßnahmen zu rechtfertigen. Mit der Weiterentwicklung technischer Erfassungsmethoden und Auswertungssysteme wird ebenso die Erfassung und Auswertung aller voranschreiten, auch ohne Anfangsverdacht oder Tatbestand.

Aber die Datenerfassung zum Schutz vor terroristischer Bedrohung ist nur ein Aspekt.

Das Abgrasen unserer Profile und Gewohnheiten findet weltweit längst schon an anderer Stelle statt: Die Wirtschaft hat ebenfalls das Potenzial der neuen Möglichkeiten für sich entdeckt. Was jedem einzelnen Menschen allein gehört, wird an Konzerne verkauft. Identitäten sind zur Ware geworden.

Auch hier setzt man zunehmend Überwachungsmethoden und dafür gebaute Technologien ein, um immer neue Erkenntnisse über den Kunden zu gewinnen und damit noch höhere Umsätze zu generieren.

Aber brauchen wir Spionagesoftware, Futuristische Bezahlsysteme und Überwachungskameras in jedem Blumenbeet, die uns überall hin verfolgen können? Alles sicher, bequem und einfach...vernetzt und zusammengeführt in großen Zentralen, wo jeder der etwas über uns wissen will, mal anfragt?

Der Kampf um unsere Daten hat gerade erst begonnen. Wie weit er in unsere Privatsphäre vordringt, wird sich in Zukunft zeigen.

** Guantanomo ist ein Synonym für ein Gefangenenlager der USA. In dem Camp auf Kuba sind vor allem Menschen inhaftiert, denen terroristische Bedrohung der demokratischen Freiheit vorgeworfen wird. Sie werden als feindliche Kämpfer bezeichnet und stehen nicht unter dem Schutz der Genfer Konvention. Für sie gelten besondere Regeln, die die Haftbedingungen ungleich härter gegenüber anderen Gefängnissen machen.*

WO STEHEN WIR JETZT?

Die Überwachung und wir.

In den letzten Monaten sind Themen, die mit Überwachung, Datenschutz und Datenmissbrauch im Zusammenhang stehen, oft durch die Medien gegangen. Viele Initiativen widmen sich dem Schutz der Privatsphäre und der Aufklärung über staatliche Vorhaben in naher Zukunft.
Es gibt heute viel mehr Möglichkeiten, sich über Gesetze, Technologien und Maßnahmen zu informieren.
Demonstrationen, die für die persönliche Freiheit und die Hoheit über die eigene Identität abgehalten werden, sind so gut besucht, wie kaum ein Protestmarsch der letzten Jahre (15.000 Teilnehmer der Veranstaltung „Freiheit statt Angst“ am 22. September 2007, geschätzte 30.000 am 11.10.2008).[2] Kritiker der „Spionagetrends“ werden in Diskussionen gern gehört. Es ist also nicht so, dass die flächendeckende Überwachung unbemerkt Einzug hält. Sie wird wohl eher mit einiger Skepsis abgewartet.
Laut einer Online-Umfrage des Fernsehsenders ARD vom 18.04.2007 (Siehe Seite 40) macht sich Bundesinnenminister Schäuble mit seinen zukünftigen Vorhaben bei den Befragten nicht besonders beliebt. Es sieht also so aus, als wäre noch mehr staatliche Kontrolle im Auftrag der Sicherheit nicht dass, was die Menschen sich wünschen. Wenn dem so ist, bleibt die Frage, warum die meisten der bestehenden Überwachungsmaßnahmen ohne größere Proteste hingenommen wurden. Liegt es daran, dass wir darüber zu wenig wissen?
Reicht uns etwa die Zusicherung, dass es nur den Schurken an den Kragen geht Ist es einfach ok, wenn Daten generiert und gespeichert werden, solange wir uns nichts zu Schulden kommen lassen?
In meiner Recherche stieß ich immer wieder auf einen passenden Vergleich:
Wenn man einen Frosch in einen Topf mit kochendem Wasser setzt, springt er sofort wieder heraus – klar, ist ja auch unangenehm. Setzt man ihn aber in kaltes Wasser, das sich langsam erhitzt, bleibt der Frosch sitzen, weil er den Unterschied nicht bemerkt. Ist das Wasser am Siedepunkt, ist es zu spät, der Frosch ist tot.[3]
Ist es das, was man mit uns versucht? Langsame Gewöhnung an die absolute staatliche Kontrolle, mit allen Mitteln, möglichst flächendeckend und im Namen der demokratischen Freiheit?
Wir sollten anfangen, uns mehr dafür zu interessieren.

Diese Arbeit wird sich vor allem mit dem Status Quo „Überwachungsstaat“ beschäftigen, zusammentragen, was gegenwärtig geschieht.
Dabei werden auch Erfahrungen einfließen, die ich selbst in diesem Zusammenhang gemacht habe.
Um zu verstehen, was unsere Gesellschaft ausmacht, wird auch der Staatbegriff betrachtet.
In einer Umfrage und einem kleinen Experiment wird sich die Einstellung der Teilnehmer zu Privatsphäre und Überwachung widerspiegeln. Staatlich eingesetzte Methoden und Maßnahmen werden vorgestellt.
Das Thema „freiwillige Überwachung“ durch Online-Communities und die neuen Möglichkeiten im Web 2.0 werden eine große Rolle spielen. Die Erkenntnisse aus dieser Bearbeitung gipfeln in meinen Interventions, (Designeingriffen). Diese sind Ausdruck meiner persönlichen Kritik an den dargelegten Umständen und machen sie ein Stück weit erlebbar.
Außerdem zeigt ein Entwurf, wie schnell ein unsichtbares Überwachungszenario geschaffen ist. Er beantwortet die Frage: Was wird uns zukünftig erwarten, wenn es uns egal ist, was mit unseren persönlichen Daten geschieht.

WO LEBEN WIR EIGENTLICH?

Was zeichnet einen Staat aus?

Das deutsche Wort *Staat* ist dem lateinischen status („Stand, Zustand, Stellung“) entlehnt. Das daher stammende italienische lo stato kam in der Renaissance auf und bezeichnete dort die mehr oder weniger stabile Verfassungsform einer Monarchie oder Republik. Der status regalis meinte Stellung, Macht und Einfluss des zur Herrschaft gelangten Königs oder Fürsten, später auch seines Anhangs, des Hofstaats. Die französische Übersetzung état konnte dann auch auf den ökonomischen Haushalt der Zentralmacht, später auch auf die rechtliche und politische Einheit aller Staatsbürger eines Staatsgebiets bezogen werden.

Ältere griechische und lateinische Begriffe wie polis (Stadtstaat), civitas („Bürgerschaft“), res publica („öffentliche Angelegenheit“), regimen („Königsherrschaft“), regnum („Königreich“) oder imperium („erobertes einheitlich regiertes Herrschaftsgebiet“) bezeichnen je einzelne, ebenfalls nicht verallgemeinerungsfähige Aspekte ähnlicher Sachverhalte.

Entscheidende Bestandteile der heute gesetzmäßigen Begriffsdeutung sind eine irgendwie geartete politische Vereinigung einer größeren Menschengruppe, die in einem mehr oder weniger geschlossenen Gebiet unter einer mehr oder weniger einheitlichen Form der – etablierten, durchgesetzten oder beschlossenen – Machtausübung leben. Diese drei Hauptkriterien haben sich im modernen Völkerrecht seit Georg Jellinek (1851–1911) herauskristallisiert.

Zum Staat gehört eine politische Instanz, die zur Schaffung und Wahrung von Recht und öffentlicher Ordnung in der Gesellschaft zuständig ist und diese mittels einer Verwaltung, dem Staatsapparat, auch durchsetzen kann.

Für Niccolò Machiavelli (1469–1527) waren alle menschlichen Gewalten, die Macht über Menschen haben, „Staat“. Für Jakob Burckhardt (1818–1897) ist der Staat damit eine der wesentlichen Kräfte neben Religion und Kultur, die die menschliche Geschichte bestimmen.

Der Staat wird oft als Gegenüber zur Gesellschaft beschrieben. [4]

Der demokratische Staat

Der wichtigste Anwendungsfall der Demokratie ist die Staatsführung. Ein Staat gilt als demokratisch, wenn die folgenden Kriterien zutreffen:

* Es gibt einen Demos (Volk), welcher politische Entscheidungen in kollektiven Prozeduren trifft.

* Es gibt ein Territorium, in dem die Entscheidungen innenpolitisch angewendet werden und in dem der Demos angesiedelt ist.

* Es gibt für politische Normen eine Entscheidungsfindungsprozedur, welche entweder direkt (z. B. als Referendum) oder indirekt (z. B. über die Wahl eines vertretenden Parlamentes) funktioniert. Diese Prozedur wird vom Demos bereits dadurch als legitimiert betrachtet, insofern sein Ergebnis „akzeptiert“ wird. In einer repräsentativen Demokratie wird die politische Legitimität der Repräsentanten aus der Bereitschaft der Bevölkerung abgeleitet, die Entscheidungen des Staates (auch die der Regierung und der Gerichte) entgegen individuellen Vorzügen und Interessen zu akzeptieren oder hinzunehmen.

* Im Fall von Nationalstaaten müssen diese souverän sein: demokratische Wahlen sind nutzlos, wenn eine Autorität von außen das Ergebnis überstimmen kann.

* Ein unverzichtbares Merkmal einer Demokratie ist schließlich, dass durch wiederkehrende verbindlich festgelegte Verfahren die Regierung ohne Revolution wechseln kann. In vorwiegend direkt-demokratischen Systemen übt das Volk die Macht selbst aus (Volksabstimmungen) In Repräsentativen Demokratien werden hierzu von den Bürgern Repräsentanten gewählt (oder in der Vergangenheit auch per Los bestimmt), die die Herrschaft ausüben sollen.

* Es existiert die Freiheit, durch eigene kreative Mitbestimmung, durch eigene Ideen, der Welt zu helfen.[5]

MOODBOARD: LOOK DER ÜBERWACHUNG

Wie sieht Überwachung aus – Eine Bildersammlung.

FILMISCHE INSPIRATION: MINORITY REPORT

Welche (Überwachungs-) Staats-Szenarien werden in Filmen aufgebaut?

Washington 2054. Die Polizei hat eine der effektivsten Waffen gegen Morde in der Hand: Ein Orakel-Dreiergespann, die Precogs, sehen Tötungen voraus. Aus Details ihrer Visionen wird der Täter zusammenspekuliert und noch bevor er die Tat begeht, festgenommen, also wegen seiner zukünftigen Morde.
Mit Hilfe dieses Systems gelang es, vorsetzliche Morde innerhalb weniger Jahre vollkommen zu eliminieren. Die Polizei operiert mit modernster Technik, um die Menschen zu finden, die im Begriff sind, ein Verbrechen zu begehen. Über jeden Einwohner gibt es eine umfangreiche Akte, die zentral abgerufen werden kann.
Durch ständige Netzhautscans, z.B. an Zugangskontrollpunkten für Gebäude oder Verkehrsmittel, ist der Aufenthaltsort eines jeden immer zu bestimmen.
Dieser Scan ist eine der Schlüsseltechnologien im Film. Er ermöglicht nicht nur die Identifikation und Erstellung von Bewegungsprofilen, sondern auch personalisierte Werbung: Wann immer jemand ein digitales Werbeplakat passiert, wird er direkt mit seinem Namen angesprochen.
Das Leben der Menschen wird durch die Scans massiv beeinflusst. Kleine spinnenähnliche Nano-Roboter werden zum Auffinden von Verdächtigen an unzugänglichen Stellen eingesetzt, um die Scans vorzunehmen. Wer sich widersetzt, macht sich verdächtig.
Werbespots für das Precrime-System versprechen, dass jeder sich auf die Unfehlbarkeit des Systems verlassen kann. Mit dem Satz „Nur ein Leben in totaler Sicherheit ist ein Leben in Freiheit“ wird jedem die Notwendigkeit für die totale Überwachung klar gemacht. Die Angst vor Kriminalität führt zu Akzeptanz.
Die Orakel werden als Mustererkennungsfilter bezeichnet, die praktisch nicht irren können. Es steht ein perfektes System einer unperfekten Gesellschaft gegenüber.
Aber es gibt immer einen Weg.
Gegen das Netzhaut-Identifikationssystem hat sich ein „Augen-Transplantations-Schwarzmarkt“ aufgebaut. In zwielichtigen Praxen kann sich jeder ein paar neue Augen einsetzen lassen.
Und auch das Precog-System hat Schwachstellen: Zum einen ist sich das Orakel-Trio nicht immer einig. Gibt es abweichende Visionen, die eine Tat nicht eindeutig vorhersehen, werden diese Abweichungen, sogenannte Minority Reports (Minderheiten-Aufzeichnungen) systematisch gelöscht, damit die Unfehlbarkeit des gesamten Systems nicht in Gefahr gerät. Zum anderen werden die grausamsten Morde, auch nachdem sie verhindert wurden, von den Orakeln immer und immer wieder gesehen.
Auch diese „Echos“ werden automatisch gelöscht.
Der Mitbegründer des Systems kennt diese Schwachstelle und nutzt sie aus, um einen Mord zu begehen. Er wird nicht entdeckt, weil er ihn aussehen lässt, wie das Echo eines geklärten Falls.

Minority Report beschreibt eindrucksvoll die Mechanismen eines Präventionsstaates (Siehe Seite 42). Und zeigt, wohin es führen kann, wenn man einer Technik uneingeschränkt vertraut.
Als der Film 2002 in die Kinos kam, wirkte er sehr futuristisch, die Technik darin faszinierend-unmöglich.
Inzwischen hat der Fortschritt aufgeholt. Einige der gezeigten multi-touch bzw. gestenbasierten Interfaces und Mechanismen wie der Netzhaut-Scan sind heute bereits nutzbar – u.a. auch, um Menschen zu überwachen.












FILMISCHE INSPIRATION: DIE INSEL

Welche (Überwachungs-) Staats-Szenarien werden in Filmen aufgebaut?

In einer futuristischen Stadt leben Menschen unter absoluter Kontrolle. Mit modernster Technik werden alle nur denkbaren Bereiche überwacht.
Die sogenannten Supervisor scannen, beobachten und erfassen jeden Einzelnen. Es ist genau vorgeschrieben, welche Kleidung die Bewohner zu tragen haben, welches Essen sie zu sich nehmen dürfen: Der körperliche Zustand ist genau bekannt und wird bei Essensausgabe überprüft. Niemand hat einen individuellen Namen, die Menschen werden in Gruppen eingeteilt. Die Gruppenbezeichnung charakterisiert Eigenschaften ihrer Mitglieder. Alle Bewohner tragen Armbänder, die persönliche Daten und Aufenthaltsort speichern, es gibt über jeden eine Personalakte, die nur von der Obrigkeit eingesehen werden kann. Niemand muss etwas selbst erledigen, es gibt jede Art von Komfort, solange keine Fragen gestellt werden. Damit die Bewohner sich nicht langweilen, verrichten sie leichte, maschinell unterstützte Arbeit, deren Sinn sich niemandem erschließt. Der direkte Kontakt von Männern und Frauen wird strikt unterbunden. Lediglich für interaktive sportliche Aktivitäten ohne Körperkontakt dürfen sie sich treffen.
Der Umstand, der die Menschen diese Maßnahmen aushalten lässt, ist erfunden: In der Welt draußen, die keiner von ihnen je gesehen hat, gab es nach Aussage der Machthabenden einen Vorfall, der die Erde kontaminiert hat. Die klinische überwachte Stadt sichert das Überleben ihrer Einwohner. Außerdem wird ein Bonussystem eingesetzt, dass die Menschen gefügig macht. Ihnen wird ihr Leben lang nur ein Ziel als erstrebenswert eingepflanzt. Sie kommen als Auserwählte auf die einzige Insel, die von der Kontamination verschont geblieben ist und als Naturparadies gilt – wenn sie das Leben in der Stadt unumwunden akzeptieren.

Eine inszenierte Lotterie entscheidet, auf wen das Los für die Insel fällt.
Wer zweifelt, bekommt die Staatsmacht zu spüren. Dann geht die Überwachung so weit, dass dem Betroffenen Nano-Roboter eingepflanzt werden, die für die Kontrolleure sichtbar macht, was der Zweifler sieht und womit er sich beschäftigt. Mit dieser Methode sollen die Quellen für das unerwünschte, selbstständige Verhalten aufgedeckt werden.
In dieser Hollywood-Fiktion wird der künstliche Staat mit allen Mitteln aufrecht erhalten, um Klone zu züchten.
Die Menschen, die in ihm leben sind Kopien von Bewohnern der normalen Welt.
Die Wissenschaft hat einen Weg gefunden, mit dieser Technik Geld zu verdienen – mit staatlicher Unterstützung. Die Organisation, die dahinter steht erzählt ihren Kunden und der Regierung, dass lediglich handlungsunfähige, gefühlstote „Fleischklumpen-Klone“ generiert werden, denen man bedenkenlos bei Bedarf Organe entnehmen kann.
Der wirkliche Zustand der Kopien unterliegt absoluter Geheimhaltung. Ebenso kennt niemand außer derjenigen, die daran Geld verdienen, die riesige Lügenmaschinerie, die angewandt wird, um die Kopien für die eigenen Zwecke gefügig zu halten.
Solange niemand Fragen stellt, ist der Klon-Staat und all seine Methoden sicher.








FILMISCHE INSPIRATION: EQUILIBRIUM

Welche (Überwachungs-) Staats-Szenarien werden in Filmen aufgebaut?

Equilibrium – The Killer of Emotions spielt in einer Welt nach dem dritten Weltkrieg. Die Überlebenden haben beschlossen, den Krieg für immer auszulöschen und den Frieden mit allen Mitteln zu erhalten.
Eine Regierungsorganisation namens Tetra Grammaton setzt sich mit militärischer Präzision und machtvollen Gesten für die Sicherheit ihrer Bürger ein. Sie gehorcht einer übergeordneten Macht – Vaters Stimme. Er ist eine gottgleiche Figur, die die Regeln des Zusammenlebens innerhalb der städtischen Gemeinschaft bestimmt hat, die moralische Instanz, mit deren Hilfe die Menschen überwacht und unter Druck gesetzt werden.
Der Schlüssel zum neu geschaffenen Frieden ist die Auslöschung aller menschlichen Gefühle. Sie werden als Quelle der Grausamkeit vergangener Zeiten angesehen. Um seine Emotion auszuschalten, ist jeder Mensch dazu verpflichtet, sich selbst täglich eine Dosis Prozium in den Hals zu injizieren. Wer sich weigert, dies zu tun, wird in einer eigens dafür gebauten Hinrichtungsmaschine lebendig verbrannt. Der Nachschub der Droge ist in staatlicher Hand.
Der Besitz persönlicher Gegenstände ist verboten. Poesie und Kunst werden ausnahmslos vernichtet. Ihr Besitz allein gilt als strafbares Individualverhalten und wird mit der Auslöschung geahndet.
Überall in der trostlosen Betonstadt werden Predigten des Vaters übertragen, der in immer gleichen Worten Gefühle verdammt und zu ihrer totalen Auslöschung aufruft. Kriegsbilder halten die grausamen Erinnerungen an die vergangenen Zeiten voller Angst und Schmerz wach und steigern die Kooperationsbereitschaft der Bürger. Uniformität und Gleichschaltung kennzeichnen die Equilibrier. Denunziantentum ist an der Tagesordnung. Jede nicht vorhersehbare Regung oder Handlung könnte den Frieden gefährden und wird deshalb selbst von Kindern gemeldet oder angezeigt. Überwachungstechnologie schließt die Lücken zur Erfassung der Lage.
Damit das gesamte System funktioniert, hat die Regierung den Grammaton-Kleriker erschaffen, einen speziellen Menschentypus, der seine Gefühle überaus gut kontrollieren kann. Seine Auffassung von Leben ist einzig, das Fortbestehen der Gesellschaft zu sichern. Mit Waffengewalt, mathematisch berechnender Kampfkunst und brutaler Attitüde sind diese Menschen eine Art Überpolizei zur Sicherung des Friedens. Jeder Kleriker besitzt die Fähigkeit, sich in die Gedankenwelt seines Gegenübers hineinzuversetzen und kann dessen Handeln und den damit verbundenen Gemütszustand präzise vorhersagen. Sie dienen, selbst unter Drogeneinfluss, loyal Vaters Stimme und werden dazu eingesetzt, sogenannte Sinnestäter aufzuspüren und zu vernichten.
Die Sinnestäter sind Menschen des Widerstandes, die sich weigern, ihre Gefühle zu töten. Sie leben verborgen im Untergrund und planen, das totalitäre Regierungssystem zu vernichten, um ihr normales Leben wiederzubekommen. Der Überwachungsstaat kommt mit wenigen Eingriffen in das Leben seiner Bürger aus. Technik kommt kaum zum Einsatz. Es wird vor allem mit psychologischen Mitteln gearbeitet.
Ideologische Prägung, große Symbole und die Abschaffung des Individuums erinnern an die Methoden des Dritten Reichs.

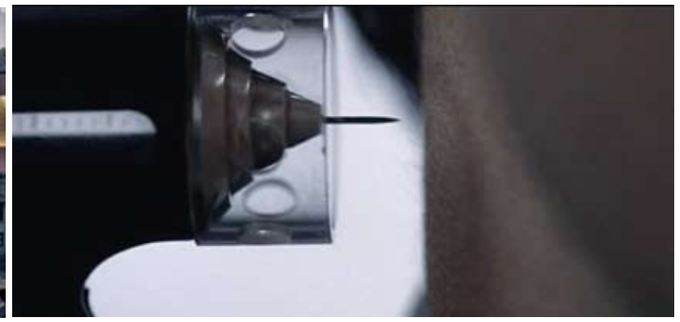












V.l.n.r.: Permanente Beschallung mit „Werbematerial“ für die Regierung. Hier für die Droge, die den Weltfrieden sichert. Einfach selbstgemacht: Injektion einer Ladung Prozium.
Konsequenz einer Straftat: Ein Sinnestäter liegt erschossen neben einem noch laufenden Plattenspieler.
Das oberste Instrument der Angst: Hinrichtung (Auslöschung) im Feuer. Eine Strafe für Menschen die nicht bereit sind, auf ihre Individualität zu verzichten und sich den Vorgaben der Regierung zu unterwerfen.

DAS „YEAR ZERO-UNIVERSUM" TRENT REZNOR/ NIN

Wie nähern sich andere gestalterisch dem Thema (Überwachungs-) Staat?

Die Nine Inch Nails (NIN), 1988 durch den Sänger Trent Reznor in Cleveland gegründet sind eine amerikanische Band, die von Beginn an nicht nur musikalische Meilensteine in der Szene gesetzt hat. Reznor begreift sich nicht als Singer/ Songwriter, sondern als Medienkünstler.
Im Studio sind weitere Musiker und Tontechniker lediglich als Assistenten gefragt, da der Sänger die meisten Instrumente selbst einspielt. Auf Konzertbühnen unterstützen ihn vier zusätzliche Musiker und bilden in diesem Moment die tatsächliche Band, in der Reznor das einzige permanente Mitglied ist. Der Musikstil wird häufig dem Industrial-Rock zugeschrieben, was aber nicht das gesamte Klangspektrum beschreibt.
Neben einem virtuosen Gefühl für Musik, dem Beherrschen aller klassischen Rockbandinstrumente und einer beachtlichen Stimme ist Trent Reznors Affinität zu moderner Technik bezeichnend für die Weiterentwicklung der Band bis heute.
Das Experimentieren mit Soundinterfaces und „Open Source-Songs" für die Fans sind fester Bestandteil des kreativen Prozesses. Der exzentrische Künstler macht am liebsten alles selbst, gegen jeden Trend, gegen jede Plattenfirma. Nach der Gründung seines eigenen Labels übernimmt er auch die Vermarktung seiner Musik, nebst Marketing und Werbung.
2007 erscheint das sechste Studioalbum „Year Zero". Es lässt zum ersten Mal das unglaubliche Potential des Künstlers in vollem Umfang sichtbar werden: In einer vorher nie dagewesenen Kampagne erschafft Reznor die Vision eines neuen Zeitalters, in dem seine Lieder zu Hymnen werden, die die Lebensumstände der Menschen im Jahre Null beklagen. Der Sänger selbst beschreibt seine Ausgangsidee zu dem Album folgendermaßen:

„Wovon es handelt? Nun, es „spielt" in einer ca. 15 Jahre entfernten Zukunft. Die Dinge sehen nicht gerade rosig aus. Wenn du dir eine Welt vorstellst, in der sich Habgier und jegliche Art von Macht so weiterentwickeln, wie man das momentan erwarten würde, dann bekommt man schon eine ungefähre Idee von der Grundstimmung des Albums. Die Welt ist an ihre eigenen Grenzen gestoßen – sowohl politisch, wie auch spirituell und ökologisch. Aus der Perspektive von diversen Charakteren, die in dieser Welt existieren, geschrieben, werden einem auf „Year Zero" diverse Blickwinkel auf eine drohende Stunde der Wahrheit präsentiert. Und wie das dann klingt? Das wirst du schon bald am eigenen Leib erfahren... " [6]

Zum Projekt
Zeitlicher Ablauf in der Realität
Offizieller Startschuss für die Kampagne war der 10. Februar 2007.
Am 12. Februar 2007 wurden markierte Buchstaben auf einem NIN Tour- T- Shirt entdeckt. Diese führten zu der Seite „iamtryingtobelieve.com"(siehe Seite 25). Dort werden Einzelheiten des Year Zero- Universums erwähnt. In den folgenden Tagen wurden insgesamt 29 weitere Webseiten entdeckt. Quellen dafür waren u.a. ID3 Tags in MP3- Dateien, die auf Konzerten gefunden wurden, Strichcodes im Booklet zum Album oder Wandgemälde in Großstädten. Für andere Seiten musste eine Telefonnummer angewählt werden, die erst durch Spektralanalyse einer Datei auf einem gefundenen USB- Stick entschlüsselt werden konnte. Eine Schnitzeljagd mit Hilfe aller erdenklichen Medien setzte Stück für Stück das inszenierte neue Weltbild zusammen. Einige Fans der Band sind vom Eintreten der Ereignisse, wie sie in Year Zero geschildert werden, bis heute überzeugt. Die letzte Seite wurde am 24. Mai entdeckt.

Zeitlicher Ablauf im Year- Zero-Universum
Das Year Zero (Jahr 0, BA 0) ist nach unserer Zeitrechnung 2022. Die Zeit davor wird als z.B. –14 (2008) bezeichnet.
Am 22. Februar wird die 81. Oscarverleihung das Ziel eines biologischen Terrorangriffs, danach werden andere Ziele in Kalifornien angegriffen. L.A. wird evakuiert. In einer Vergeltungsaktion werden im März Iran und Nord- Korea von den Amerikanern mit Nuklearwaffen angegriffen. Die Beweise für die Schuld dieser Länder am Biowaffenangriff sind jedoch nicht schlüssig.
Im August 2009 erklären Moslems weltweit den Jihad gegen die USA.
Ab September wird das Trinkwasser in Amerika flächendeckend mit Parepin versetzt, einem Psychopharmaka. Der Bevölkerung wird allerdings erklärt, dass Parepin als Schutzmaßnahme vor Bioterrorismus dient. Menschen, die kein Trinkwasser aus der Leitung trinken und bei klarem Verstand sind, gelten als paranoid.
Freie Rede wird verboten, Protestler werden inhaftiert und exekutiert.
Im Jahre 2013 zerbrechen die Regierungen in Afrika, ohne dass die Hilferufe der Afrikanischen Union gehört werden.
2015 hat der Indisch- Pakistanische Krieg die gegenseitige Auslöschung beider Länder zur Folge.
Ein brutaler Überfall Krimineller während der Fußball- WM 20018 in Großbritannien hat die elektronische Kennzeichnung auffällig gewordener Bürger zur Folge. Dies geschieht durch die Implantierung eines Nerochips ins Handgelenk.
Die erste amerikanische Präsidentin wird wegen Hochverrats des Amtes enthoben. Danach werden freie Wahlen abgeschafft

Eine andere Version der Wahrheit. Durch das Hin-und Herwischen mit der Maus auf der Webseite legt der Betrachter das wahre Gesicht des neuen Amerika frei.

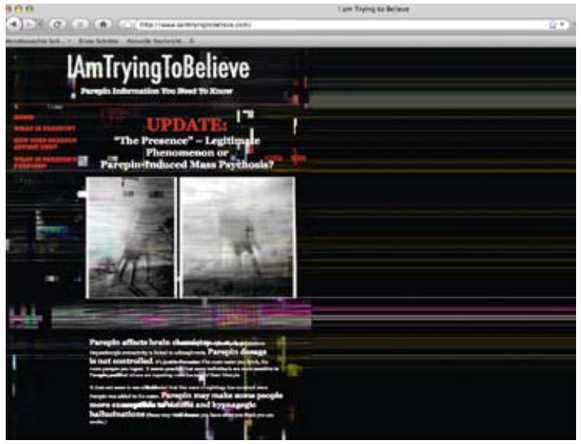
und der Präsident vom Kongress ernannt. 2019 inszeniert die amerikanische Regierung angeblich einen bioterroristischen Anschlag auf Seattle um die Notwendigkeit von Parepin zu untermauern. Der Tod eines US- Diplomaten in Algerien am Kampfvirus „Redhorse“ führt zu einer weiteren Beschränkung der Bürgerechte. 2021 bilden internationale Großkonzerne und Weltregierungen die Koalition für Frieden. In 2022 (Jahr 0) führt Amerika zusammen mit der Koalition für Frieden eine neue Zeitrechnung ein. Am 2. August 2022 fangen Widerstandsgruppen an, Nachrichten übers Internet in die heutige Zeit zu senden, um auf die Umstände in der Zukunft aufmerksam zu machen. In den Jahren 2020 bis 2022 ersetzt die Droge Opal, eine stärkere „Straßenversion“ von Parepin, Kokain. Am 2. Oktober 2022 erscheint die „Presence“ über dem Kapitol in Washington D.C. Eine Erscheinung in Form einer (göttlichen) Hand, die vor allem durch die Einnahme von Parepin bestärkt wird. Das von der Regierung inszenierte Phänomen wird on den Menschen als Drohung gegen falscvhes Leben, also Andersdenken und Auflehnung gegen den Staat verstanden.

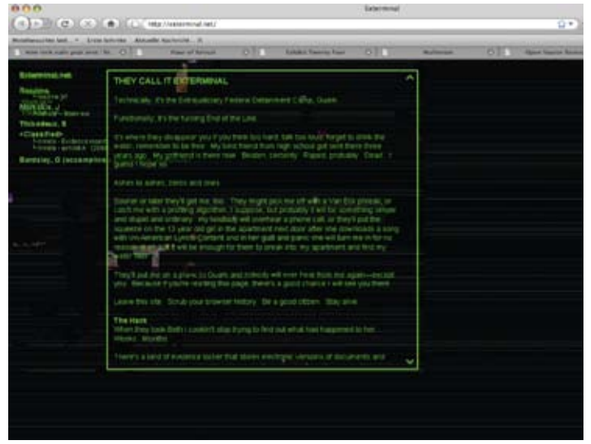
Technik Im Year- Zero Universum

Es gibt relativ wenig technische Neuerungen. Die konsequente Anwendung heutiger Technik und Möglichkeiten Menschen zu überwachen und zu kontrollieren ist der Schlüssel des fiktiven Staates. Neu ist, dass Kriminellen oder auffälligen Bürgern ein sogenannter Nerochip ins Handgelenk eingepflanzt wird. Dieser dient der ständigen Überwachung, mögliche Zusammenkünfte sollen verhindert werden. Bürger, die sich die Chips wieder entfernen (Chip-Puller) werden gnadenlos gejagt und inhaftiert. Weiterhin werden Kameras zur Überwachung eingesetzt. Der Großteil der Überwachung ist allerdings eher psychologischer Natur. Die Droge Parepin im Trinkwasser verändert das Bewusstsein der Menschen, sie werden apathisch. Dadurch können die Bürgerrechte weitestgehend eingeschränkt werden.

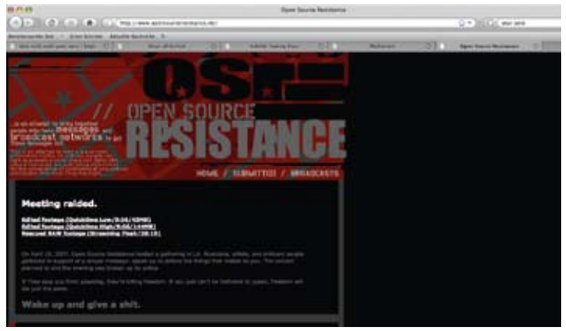
Konzept und Design

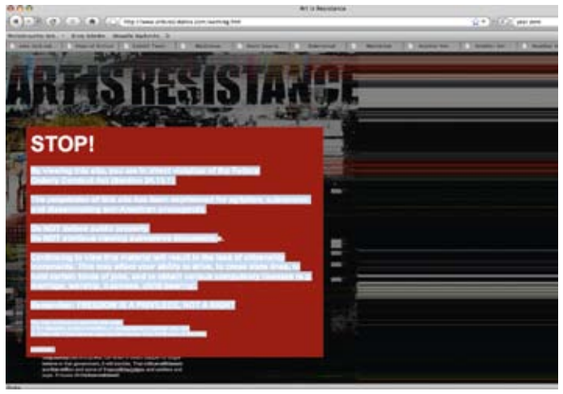
Das globale Szenario wird indirekt erklärt. Fragmentarisch findet man Hinweise in den Liedtexten der Platte „Year- Zero“, in verteilten Comics, Tagebuchnotizen, Fotos, E- Mails, Transkripten von Gesprächen, Telefonanrufen und Wandgemälden.
Vor allem auf den versteckten Webseiten erwecken Bruchstückhafte Meldungen und Erinnerungen aus einer anderen Zeit den Eindruck einer existierenden Parallelwelt. Entdecker der Informationen bekommen kein genaues Bild der zukünftigen Zustände, sind aber zum Handeln gegen die Anfänge in unserer Zeit aufgerufen.
Der Sänger bringt seine Fans dazu, ihre Stimme gegen Ungerechtigkeit und Ausbeutung zu erheben und zeigt dabei auf die heutige US-Regierung.
Eine der entdeckten Seiten hält Material für erste Street- Art und Protestaktionen bereit. Im Laufe der Zeit werden verschiedene Aktionen von den Fans selbst organisiert. Für viele ein Höhepunkt der Kampagne: ein exklusives NIN- Live- Konzert in einer verlassen Werks- Gegend in L.A.
Um zu diesem „konspirativen Treffen“ zu gelangen, wurden online Hinweise gegeben, wo in L.A. Handys zu finden sind, die zu einem bestimmten Zeitpunkt angerufen werden.
So erhielten Fans weitere Instruktionen. Das Konzert wurde nach 6 Liedern von verkleideten SWAT- Einheiten gestürmt und die Besucher aus der Halle gejagt.
Dieses Konzert fand sowohl in Echtzeit als auch im Year- Zero Universum statt. Es gilt als verbindendes Element beider Welten. Trent Reznor ist Kopf der Widerstandbewegung, heute und in der Zukunft.





Eine Kampagne, die ihresgleichen sucht:
Mit allen Mitteln promoted Trent Reznor sein Album „Year Zero“. Communities und Blogs nutzt er für die glaubhafte Verbreitung von Zeitzeugenmaterial seiner Überwachungsstaat-Utopie.





Links: Einige der Websites aus dem „Year Zero“- Universum. Aus den Bereichen Medizin, Umweltschutz und Kultur erreichen Eindrücke unsere Welt. Abgerundet werden sie durch private Homepages, Material der Widerstandsbewegung und diverse Blog-Einträge.
Oben: Screenshots aus dem offiziellen Trailer zu Year Zero. In verzerrten Bildern ist die „Presence“ zu sehen, die die Bürger des fiktiven Staates in Atem hält.

BANKSYS KRITISCHE STREET ART

Wie nähern sich andere gestalterisch dem Thema (Überwachungs-) Staat?

„He is the Scarlet Pimpernel* of modern art, so adept at leaving false trails that even his own agent has claimed that he is not certain of his identity.“ („Er ist das Scharlachrote Siegel der Moderen Kunst, so darauf bedacht, falsche Spuren zu legen, dass selbst sein Agent nicht sicher seine Identität kennt“). [7]

Tatsächlich ist die wahre Identität Banksys immer noch nicht geklärt. Seine Werke hängen im MoMA, Tate Modern und Metropolitan Museum of Art in New York City. Sie bringen Händlern Millionen. Wände, die er verschönert hat, werden abgetragen und konserviert. Er ist Englands berühmtester Street-Art-Künstler und sorgt weltweit für Furore. Doch wer er wirklich ist, liegt im Dunkeln. Es wird vermutet, dass er 1974/75 in Bristol geboren ist. Sein richtiger Name könnte Robin Banks sein, oder Robin Gunningham...[8]
Genau das ist es, was das Faszinatum Banksy am Leben hält, Teil seiner Methode. Er ist Meister im Spuren verwischen. Damit bewegt er sich genau entgegen der Umstände, die er anprangert. Viele seiner Werke üben Kritik an der Überwachunspolitik Englands. Mit einem für ihn typischen Humor, behandelt er ernste Inhalte. Ungeniert besprüht er Wände – beobachtet oder nicht. Er will wachrütteln, für wirtschaftliche und politische Themen sensibilisieren. Dabei ist seine Sicht auf die Dinge immer ein Alternativangebot an sein Publikum. Typisch für seinen Stil ist sowohl die Veränderung klassischer Motive, als auch die Kreation von Schablonenbildern.

Bei seinen Arbeiten bedient er sich der Taktiken der Kommunikationsguerilla, die im folgenden so charakterisiert werden:

Kommunikationsguerilla (auch Informationsguerilla, Medienguerilla) ist eine Form des Aktivismus (bzw. eine Gruppe oder Bewegung, die sich dieser Form bedient), bei der gezielt Information bzw. Desinformation eingesetzt wird, um Ziele zu erreichen. Dabei wird die klassische Guerilla-Taktik, die sich um möglichst effektive punktuelle Operationen bemüht, auf den Bereich von Information und Kommunikation übertragen. Man kann die Kommunikationsguerilla auch als eine künstlerische Strategie zur Subversion von Kommunikationsstrukturen oder eine kulturelle Instandbesetzung beschreiben. Verwandte Begriffe sind auch Adbusting und Culture Jamming. [9]

Banksy zeichnet keine direkte Überwachungsstaat-Utopie, er macht den Status Quo diesbezüglich, vor allem in London sichtbar. Er vermittelt den Menschen mit seinen Werken einen visuellen Eindruck für ihre momentane Situation. Und er stellt frei, sich Gedanken darüber zu machen, ob man daran in Zukunft etwas ändern sollte. Damit sind seine Graffitis nicht nur zweidimensionale Bilder, sondern greifen als Interventionen in die Lebensumstände einiger Städte(r) ein.

** The Scarlet Pimpernel, dt. Das Scharlachrote Siegel ist ein Musical nach dem gleichnamigen Roman von Emmuska Orczy. Es spielt während der Französischen Revolution und erzählt die Geschichte eines englischen Adeligen, der maskiert unter dem Decknamen „Das scharlachrote Siegel“ gegen die grausame Regierung kämpft und zahlreiche Menschen von der Guillotine rettet. Niemand weiß, wer er wirklich ist.* [10]

Haushohe Paintings, direkt neben einer Überwachungskamera – typisch für Banksy.

Eine Auswahl von Banksys Werken zum Thema Überwachung. V.l.n.r.: Ironische Kunst, die alt und neu vereint. Idyllisches Landschaftsgemälde mit Rundum-Überwachung. Nur für den Fall...
Eines seiner bekanntesten Motive; Eine Überwachungskamera starrt eine kahle Betonwand an. Ein Grund für den Künstler, sie und sich zu fragen „Was überwachst du?“
Von der britischen Banksy-Homepage, Rubrik What Happened Next (Was als nächstes passierte): Kritik an der Kritik; Banksys Avatar, die Ratte ziert ausgerüstet mit Richtmikrofon und Aufnahmegerät eine Häuserwand. Direkt unter dem Schild der Vereinigung für Gehörlose kam diese doppeldeutige Satire nicht gut an – das Kunstwerk UND das Schild wurden entfernt.

DAGEGEN: „STASI 2.0" DIRK ADLER U.A

Wie nähern sich andere gestalterisch dem Thema (Überwachungs-) Staat?

Der Begriff Stasi 2.0 stammt aus der Netzkultur. Er setzt sich aus zwei Bestandteilen zusammen: Zum einen „Stasi"= Staatssicherheit – ein Verweis auf das Ministerium für Staatssicherheit der ehemaligen DDR. Zum anderen „Web 2.0", ein Schlagwort, das für die Weiterentwicklung neuester Internet-Technologien und deren Möglichkeiten steht. Zusammengesetzt kritisiert Stasi 2.0 den drohenden Überwachungsstaat Deutschland und die damit einhergehende Bedrohung digitaler Bürgerrechte. Der Begriff dient als Symbol für die Opposition gegen umfassende Datenspeicherung durch die Bundesregierung. Der Protest richtet sich gezielt gegen den Bundesinnenminister Wolfgang Schäuble und die von ihm veranlassten oder vorgeschlagenen Maßnahmen. Darunter finden sich zum Beispiel die Online-Durchsuchungen privater Computer, Vorratsdatenspeicherung oder nicht technisch bedingte Maßnahmen wie die von der Staatssicherheit der DDR bekannte Sammlung von Geruchsproben und dem Unterbindungsgewahrsam. Die Auflehnung gegen seine Politik wurde vor allem 2007 im Vorfeld des G8-Gipfels in Heiligendamm deutlich, anlässlich dessen der Innenminister einige seiner umstrittenen Vorschläge unterbreitete, um den drohenden Gipfelprotest zu unterbinden.
Aufgrund seiner entschiedenen Haltung und der beschriebenen Gründe ist Wolfgang Schäuble das Gesicht zu Stasi 2.0. Das Logo der Kampagne ist eine Sprühschablone im Street-Art-Stil, „Schäublone" genannt. Entwickelt wurde sie vom Medieninformatiker Dirk Adler. Das Weblog dataloo veröffentlichte sie erstmals. Darauf folgten die „Platterone", ein Motiv mit dem österreichischen Innenminister Günther Platter und Schablonen von 19 weiteren Politikern. Außerdem wurde für die Kampagne eine eigene Schrift entwickelt.

Protestaktionen
Unter dem Motto Stasi 2.0 mit der Schäublone als Wiedererkennungsmerkmal finden deutschlandweit Aktionen gegen die genannte Sicherheitspolitik statt. Zum ersten Mal wurde der Begriff im Rahmen einer Kunstaktion am 18.April 2007 vor dem Reichstag benutzt, während das Bundeskabinett den Entwurf zur Vorratsdatenspeicherung beschloss. Auf großformatigen Schildern wurden sensible Informationen zu den Demonstranten für jeden sichtbar zur Schau gestellt, um auf die Folgen des Regierungsbeschlusses aufmerksam zu machen (Siehe Seite 39). Auf der IFA 2007 in Berlin wurden Transparente mit dem Stasi 2.0-Logo während eines spontanen Go-Ins von Mitgliedern des Arbeitskreises für Vorratsdatenspeicherung und dem Chaos Computer Club (CCC) über dem Stand der Deutschen Telekom aufgehängt. Damit spielten die Protestler auf einen bekanntgewordenen Skandal innerhalb des Konzerns an, bei dem Sicherheitsmitarbeiter Verbindungsdaten zwischen einem Journalisten und einem Aufsichtsratsmitglied ausspioniert und Gespräche abgeglichen hatten.[11] Die bisher größte Aufmerksamkeit bekam die Protestaktion auf der

** Volkszählungsboykott 1987, Eine Bewegung gegen die Volkszählung, die zwischen 1983 und 1987 zum Volkszählungsboykott aufrief, mahnte die Einhaltung grundgesetzlicher Rechte und Bestimmungen des Datenschutzes an. Eine 1983 geplante Volkszählung wurde durch eine Grundsatzentscheidung des Bundesverfassungsgerichts zum Datenschutz und dem Recht auf informationelle Selbstbestimmung (Siehe Seite 42) verhindert. Daraufhin wurden die Fragebögen so modifiziert, dass die Beantwortung der Fragen möglichst keine Rückschlüsse auf die Identität der Befragten zulassen sollte.*[12]

Die Stasi 2.0-Schäublone.

Demonstration „Freiheit statt Angst“ am 22.September 2007 in Berlin.
Unter massiver Präsenz der Sprühschablone auf Stickern, Schildern und Shirts protestierten etwa 15.000 Menschen für Bürgerrechte und Datenschutz. Die Veranstaltung gilt als die bis dahin größte Protestaktion seit dem Volkszählungsboykott 1987.* Am 11. Oktober 2008 bewegte sich ein weiterer Demonstrationszug durch Berlin. Die Veranstalter zählten etwa 30.000 friedliche Teilnehmer.[2]

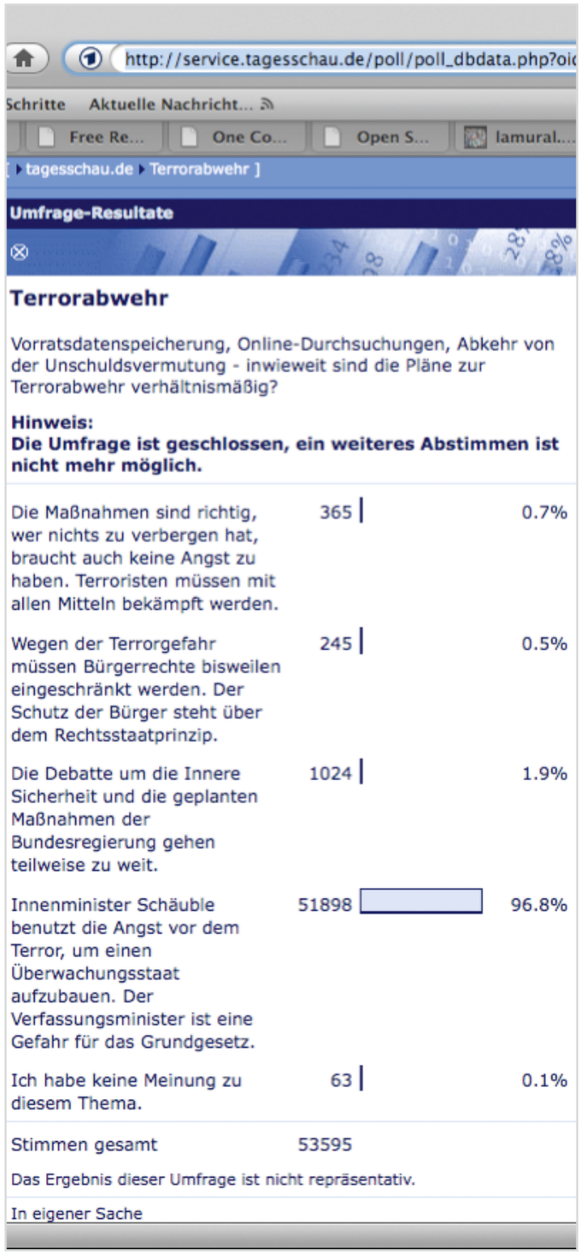
Kritiker
Einige Kritiker betrachten die Bezeichnung als unangemessene Überspitzung und unzulässige Verharmlosung des Ursprungsbegriffs Stasi, auch im Hinblick auf deren Opfer. Andere Stimmen bezeichen das Ziel der Kampagne als zu sehr auf einzelne Politiker fixiert. Dabei würde die der Politik zugrunde liegende Kontrollmentalität in der Gesellschaft nicht berücksichtigt werden. Demnach gebe es nicht nur die Interessen des Staates nach Kontrolle, sondern auch eine „Blockwart“-Mentalität innerhalb der Gesellschaft: „Wer in der Zeitung über seine Nachbarn lesen will, was sie für sexuelle Gepflogenheiten haben oder wie gemeinschaftsfeindlich sie sich der unkorrekten Mülltrennung schuldig machen, der hat wenig Skrupel, was einen starken, schützenden Staat angeht.“ Zu einer kritischen Betrachtung gehöre auch die Frage, welche Maßnahmen besonders wenig Beachtung in der Gesellschaft erfahren, zum Beispiel bei der geräuschlosen „Erweiterung des kleinen Bundesgrenzschutzes zur riesigen Bundespolizei“. Angesprochen wird dabei die Mentalität in der Gesellschaft gegenüber „Fremden“ und „Minderheiten“ wie Einwanderern.[13]

Gegenwind und andere Vorfälle
Im August 2007 wurde ein Informatik- Student, der das Motiv Stasi 2.0 sichtbar auf seinem Auto mit sich führte, von der Polizei wegen anfänglichem Verdacht auf Beleidigung angezeigt, das Bild beschlagnahmt und der Fall an die Münchner Staatsanwaltschaft weitergeleitet. Das Verfahren ist im Oktober 2007 eingestellt worden. [14]
Unter Fußballfans wird die Schäublone zunehmend zum Sprachrohr ihrer Verstimmung. Grund dafür ist, dass in den letzten Jahren die systematische Überwachung und Datenerfassung der sogenannten Ultra-Fans und Hooligans zugenommen hat, um vor allem bei Großereignissen wie der Weltmeisterschaft Randalen zu begegnen und bekannte Störer polizeilich von Spielen auszuschließen. Im November 2007 brachten einige Fans des Fußballvereins 1. FC Union Berlin im Stadion ***An der Alten Försterei*** mit einer Schäublone im Großformat ihren Unmut über zunehmende Überwachung der Fußballfans zum Ausdruck. Um angekündigte Konfrontationen mit den Polizeikräften zu vermeiden, forderte der Ordnungsdienst des Vereins die Fans unter Androhung von Hausverbot auf, besagte Transparente zu entfernen, worauf diese mit einem weiteren Transparent mit der Aufschrift „Freie Meinungsäußerung?“ reagierten und anschließend geschlossen das Stadion verließen. Der 1. FC Union entschuldigte sich daraufhin bei den betroffenen Fans und gab an, dass der Ordnungsdienst falsch und überzogen reagiert hatte.[15]

Links: Die Schäublone im Einsatz.
Oben: Kunst, die aufmerksam macht: Die Schilder, die „sensible Daten“ ihrer Träger an die Öffentlichkeit bringen. Hier bei einer Aktion in Bremen.

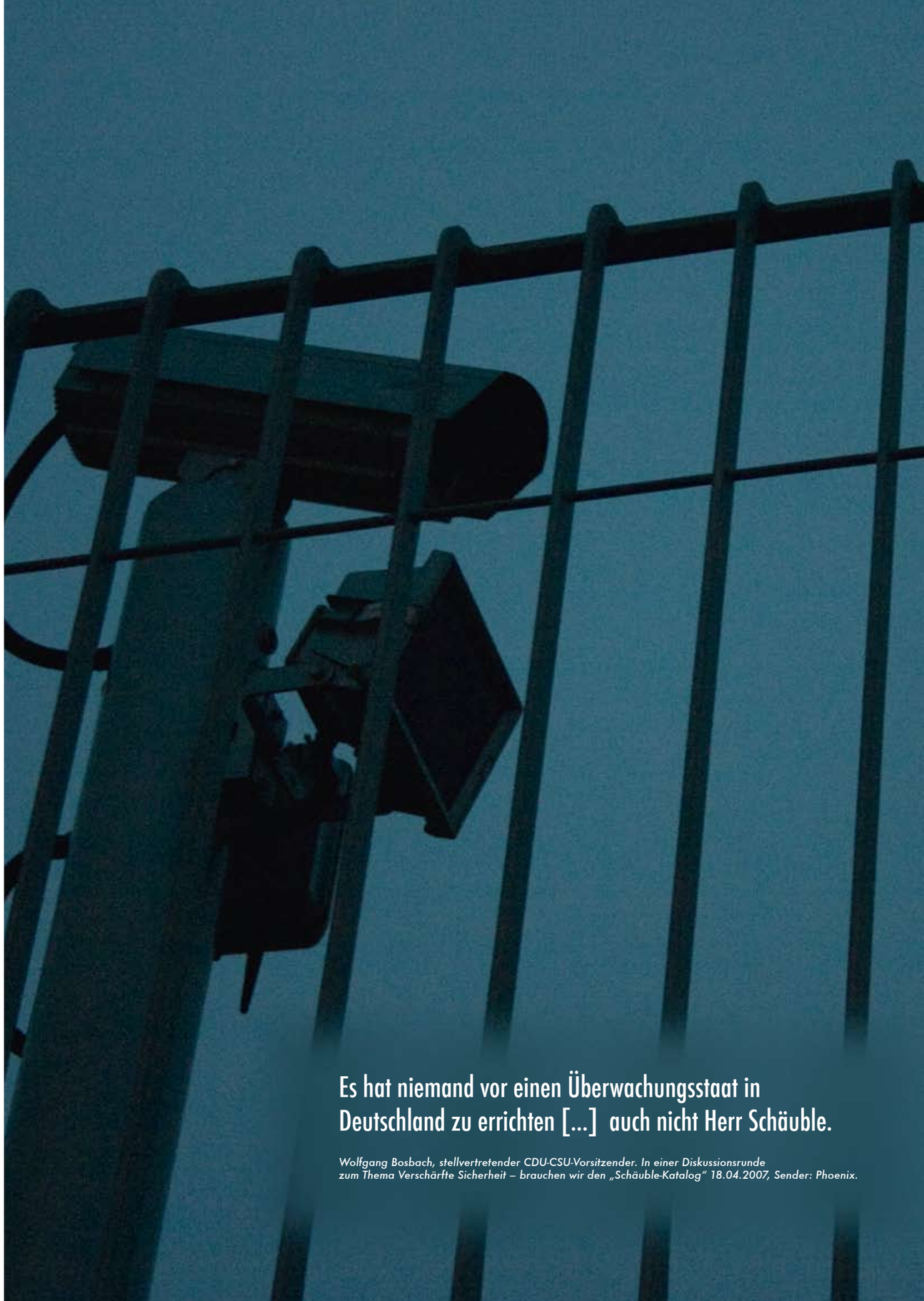
ANDERE HABEN AUCH MAL GEFRAGT

Eine Umfrage zum Thema Terrorabwehr mittels Überwachungsstaat.



Eine online-Umfrage der ARD Tagesschau vom 18.04.2007:
Das Ergebnis ist eindeutig. 97% der Teilnehmer befürchten den Aufbau eines Überwachungsstaates durch Innenminister Schäuble mit allen Mitteln. Ein ungewöhnlich hohes Ergebnis. Einen Tag später hatte man festgestellt, dass es manipuliert worden war: Einige Teilnehmer nahmen offensichtlich mehrere tausend Mal an der Umfrage teil, durch automatisierte Zugriffe.
„Daher bereinigten wir die Umfrage umgehend: Jede IP-Adresse wurde nur noch einmal zugelassen - was allerdings auch einer Manipulation entspricht. Denn so kann beispielsweise aus Großbetrieben jeweils nur eine Stimme abgegeben werden.
Das Ergebnis bleibt dennoch eindeutig: Danach stimmten mehr als 11.000 Teilnehmer für die oben aufgeführte Antwort.“[16]

Dieses Beispiel zeigt eindrucksvoll zwei Dinge. Erstens: Wenn die Kommunikationskanäle nicht genügend gesichert sind, gibt es immer einen Weg, gutmütig abgegebene Informationen für die eigenen Belange zu verfälschen und damit den eigentlichen Zweck zu verfremden oder zu gefährden. Zweitens: In der Bevölkerung wächst die Angst vor zunehmender Überwachung durch den Staat. Allerdings ist ein großer Nachteil von Online-Umfragen, dass nur die Leute daran teilnehmen, die technisch ausgerüstet sind. Das schließt also einige Gruppen aus, deren Antwort das Ergebnis beeinflusst hätte.
Um mir meinen eigenen Eindruck der gängigen Meinung zu diesem Thema zu verschaffen, habe ich selbst eine Umfrage durchgeführt (Siehe Seite 50).



Es hat niemand vor einen Überwachungsstaat in Deutschland zu errichten [...] auch nicht Herr Schäuble.

Wolfgang Bosbach, stellvertretender CDU-CSU-Vorsitzender. In einer Diskussionsrunde zum Thema Verschärfte Sicherheit – brauchen wir den „Schäuble-Katalog“ 18.04.2007, Sender: Phoenix.

ÜBERWACHUNSSTAAT VERSUS PRÄVENTIONSSTAAT

Was kennzeichnet einen Überwachungsstaat und wo ist der Unterschied zum Präventionsstaat?

Der Begriff *Überwachungsstaat* beschreibt ein Szenario, in dem ein Staat seine Bürger mit allen zur Verfügung stehenden und staatlich legalisierten Mitteln überwacht. So sollen Gesetzesverstöße besser und schneller erkannt und verfolgt werden können. Befürworter führen die Verhinderung von Straftaten, organisierter Kriminalität und Terrorismus als Notwendigkeit für die Etablierung einer umfassenden Überwachung der Bürger an. Kritiker halten einen Überwachungsstaat hingegen für nur schwer oder gar nicht mit einer freiheitlichen Demokratie vereinbar. Im Überwachungsstaat werden die Erkenntnisse aus der Überwachung hauptsächlich zur Verhinderung und Ahndung von Gesetzesverstößen, sowie zur Gewinnung von geheimdienstlichen Informationen über die einzelnen Individuen und Bevölkerungsgruppen genutzt. Die Prävention von Straftaten und anderen unliebsamen Verhaltensweisen der Bürger findet im Überwachungsstaat bereits indirekt durch den ständigen Beobachtungsdruck statt. In diversen überwachenden Staaten waren bzw. sind „präventive“ Festnahmen überwachter Personen vor Veranstaltungen üblich, um das öffentliche Erscheinungsbild der Veranstaltungen zu beeinflussen (China, Nepal, Kolumbien, DDR, UdSSR).
Auch in der Bundesrepublik Deutschland wurden gewaltbereite Störer präventiv in Haft genommen, z.B. während des G8-Gipfels in Heiligendamm 2007.
Der Überwachungsstaat zeichnet sich durch die Einschränkung des Datenschutzes, der Privatsphäre und der informationellen Selbstbestimmung* aus.
Als Beispiele für typische Maßnahmen des Überwachungsstaates seien Rasterfahndungen, Kameraüberwachung öffentlicher Plätze, die routinemäßige Erstellung von Bewegungsprofilen, Gendatenbanken (Genetischer Fingerabdruck), biometrische Datenbanken, umfassende Kommunikationsüberwachung, sowie die Schleppnetz- und Schleierfahndung und die ab 1. Januar 2008 in der EU und damit auch Deutschland gestartete Vorratsdatenspeicherung genannt. [17]

** Informationelle Selbstbestimmung: Dieses Grundrecht ist eine Ausprägung der Menschenwürde (Art. 1 I GG) und der allgemeinen Handlungsfreiheit (Art. 2 I GG) und besagt, dass jeder grundsätzlich selbst darüber entscheiden kann, ob er personenbezogene Daten preisgibt. Als personenbezogene Daten bezeichnet man Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Alle Informationen und Umstände, mittels derer man den Bezug zu einer konkreten Person herstellen kann, sind folglich solche personenbezogenen Daten. Hierzu gehören auch Daten die öffentlich oder einem größeren Personenkreis zugänglich sind, wie die Telefonnummer oder das Kfz-Kennzeichen.* [18]

Ein *Präventionsstaat* ist ein Staat, welcher die ihm zur Verfügung stehenden Informationen aus diversen Überwachungseinrichtungen massiv einsetzt, um unerwünschtes Verhalten der Bürger von vornherein zu verhindern. Der Präventionsstaat ist die logische Weiterentwicklung des Überwachungsstaates. Im Überwachungsstaat werden die Erkenntnisse aus der allgegenwärtigen Überwachung noch größtenteils zur nachträglichen Ahndung von Gesetzesverstößen und zur Gewinnung von geheimdienstlichen Informationen über die einzelnen Individuen und Bevölkerungsgruppen genutzt.
Im Präventionsstaat hingegen werden die Informationen aus den Überwachungsmaßnahmen bereits benutzt, um Gesetzesverstöße oder unliebsames Verhalten von vornherein zu verhindern. Als Beispiele für typische Maßnahmen des Präventionsstaates seien Demonstrationsverbote, Platzverweise, Aufenthaltsverbote, Meldepflichten, Berufsverbote, Ausweisungen unliebsamer Personen, Rasterfahndungen, umfassende Kommunikationsüberwachung, Sicherungsverwahrungen, Unterbindungsgewahrsam, Schleier- und Schleppnetzfahndungen, sowie massive verdachtsabhängige und verdachtsunabhängige Kontrollen durch diverse Behörden und die Polizei genannt.
Darüber hinaus zeichnet sich der Präventionsstaat durch die Minimierung des Datenschutzes, der Privatsphäre und der informationellen Selbstbestimmung aus. Die Überwachungsdaten aus allen Bereichen werden im Präventionsstaat zu umfassenden persönlichen Profilen in großen Datenbanken kombiniert. Hierdurch ist ein effizientes Durchsuchen nach bestimmten Mustern zum Zwecke der Prävention möglich. Fürsprecher des Präventionsstaates halten diesen angesichts der Gefahren des Terrorismus für notwendig und sinnvoll. [19]

VORRATSDATENSPEICHERUNG
E-MAILUEBERWACHUNG
GROSSER LAUSCHANGRIFF
RFID-CHIPS
VERMUMMUNGSVERBOT
VIDEOUEBERWACHUNG
ELEKTRONISCHER REISEPASS
FINGERPRINTSCAN
BIOMETRISCHE GESICHTSERKENNUNG
STEUER-IDENTIFIKATIONSNUMMER
ECHELON
BKA-GESETZ
FRA-GESETZ
ZENTRALES MELDEREGISTER
STAATLICHER KONTENABRUF
AUTOMATISCHE NUMMERNSCHILDERKENNUNG
MAUTDATENERHEBUNG
ANTITERRORDATEI
ELEKTRONISCHE GESUNDHEITSKARTE
OBSERVATION
EINLADERDATEI
GERUCHSPROBEN
STILLE SMS
FLUGDATENWEITERGABE
TELEFONUEBERWACHUNG
SCHUFA AUSKUNFT
MUSTERERKENNUNG
RASTERFAHNDUNG
OHNE DURCHSUCHUNGEN
VORRATSDATENSPEICHERUNG
E-MAILUEBERWACHUNG
GROSSER LAUSCHANGRIFF
RFID-CHIPS
VERMUMMUNGSVERBOT
VIDEOUEBERWACHUNG
ELEKTRONISCHER REISEPASS

STAATLICHE MASSNAHMEN

Wie sieht die gegenwärtige Situation aus?

Maßnahmen	Beschreibung und Einsatzmöglichkeit	Verbreitung	Personalaufwand	Gefährdung d. gen. Daten
Kameras	Visuelle Erfassung von Personen innerhalb des Aufnahmeradius. Zoom auf Details möglich. Speicherung des Materials.	●●●○	●●○○	●○○○
DNS-Tests	Zur Eingrenzung einer ver dächtigen Gruppe eingesetzt, wenn DNS-Spuren während der Aufklärung eines Verbrechens sichergestellt wurden. Sicherung der Proben in einer Datenbank.	●●○○	●●●○	●○○○
Datenspeicherung	Aufzeichnung und Speicherung von Kommunikationsvorgängen (Protokolldaten) durch Provider.	●●○○	●○○○	●○○○
Online-Durchsuchung	Nicht nachweisbare Durchsuchung von privaten Computern nach verdächtigen Dateien (Keyword-Suche). Übermittlung und Speicherung relevanter Inhalte.	●●○○	●●●○	●●○○
RFID-Chips	Funkchip, der beliebige voher gespeicherte Daten tragen kann. Sein Inhalt wird unbemerkt über ein Lesegerät angezeigt.	●●●●	●○○○	●○○○
Maut-System	Visuelle Erfassung von KFZ-Kennzeichen durch Kameras. Erstellung von Bewegungsprofilen relevanter Fahrzeuge.	●●●○	●●○○	●○○○
Digitaler Fingerabdruck	Abdruckerfassung durch Scan. Speicherung in einer Datenbank zur sicheren Zuordnung biometrischer Daten zur Person.	●●○○	●●●○	●○○○
Gesichtserkennung	Visuelle Erfassung von Gesichtszügen via Infrarot. Erstellen eines 3D-Abbildes. Detailgetreue Modellierung möglich.	●●○○	●○○○	●●○○
Abhören	Einwählen in Telefongespräche, Aufzeichnen von Verbindungen, Stimmproben und Inhalten.	●●●●	●●●●	●○○○
Trojaner	Über das Internet unbemerkt verbreitete Software zur automatischen Übermittlung von Daten (z.B. an das BKA) privater Computer, die den Trojaner tragen.	●●●○	●●●○	●○○○
Observation	Überwachung verdächtiger Personen mittels verdeckter Ermittler. Bei der Observation können Bewegungsprofile, Kontaktpersonen, Kommunikation und die unmittelbare Umgebung genau erfasst werden.	●●●○	●●●●	●○○○

Legende

- ● hoch
- ○ niedrig
- ●○○ hoch
- ●○○ hoch

Die hier aufgeführten Maßnahmen sind die gängigsten Methoden in der kriminalistischen Arbeit. Sie sind den meisten Bürgern bekannt, da auch in den Medien oft darüber berichtet wird.

ÜBERWACHUNG HOLLYWOODREIF

Was kommt eigentlich noch?

Vor drei Jahren stand ich auf dem Flughafen Newark in New Jersey (USA) in der Warteschlange für Einreisende aus den EU-Staaten. Zu diesem Zeitpunkt hatte ich folgende Erfahrung mit den erhöhten Sicherheitsbestimmungen bereits hinter mir. Vor dem Abflug wurden meine Koffer zweimal geöffnet und durchsucht. Mir wurde eine Schachtel Streichhölzer abgenommen. Ich bin durch unzählige Kontrollen, Schleusen, an Sicherheitsbeamten und Metalldetektoren vorbei gegangen. Habe wann immer man mich fragte, meine Jacke ausgezogen, meine Hosentaschen geleert, meinen Gürtel abgelegt und meine Schuhe ausgezogen. Im Flugzeug füllte ich ein verwirrendes Dokument über meine Einreisegründe aus. Am Zoll wurde ich zu mitgebrachten Waren befragt...
Das alles war nicht weiter dramatisch, sehr lästig, aber irgendwie zu verstehen.
Als ich an der Reihe war, dem freundlichen US-Beamten meinen Pass auszuhändigen, passierte etwas, dass ich erst viel später vollends begriff. Als erstes wurde mein Pass gescannt und mein Foto mit mir verglichen. Klar, das machen die überall. Nachdem ich den Einreisestempel bekomme hatte, bat mich der Beamte, einen Moment unbewegt in eine bestimmte Richtung zu schauen. Klick. Aha, ein Foto. Danach legte ich noch meinen Finger auf ein kleines Gerät. Zweimal, denn der erste Fingerabdruck-Scan war nicht gut gelungen. Während das alles passierte, unterhielt sich der wirklich sehr nette Beamte ganz ungezwungen mit mir: Was denn der Grund für meinen Besuch sei, wie lange ich bliebe, wohin ich weiterreiste...
Er war entzückt davon, dass ich meine Schwester besuchen wolle und wünschte mir viel Spaß. Wow! Nach neun Stunden Flug war ich echt begeistert von solch einem herzlichen Empfang. So was kennt man aus Deutschland gar nicht, dachte ich damals noch.
Einige Zeit später hörte ich von den allgemeinen Sicherheitsmaßnahmen an amerikanischen Flughäfen: Pass-Scan, Fingerabdruckerfassung, Foto zum Zeitpunkt der Einreise und Aufzeichnung einer Stimmprobe während eines netten Gespräches am Schalter. Alles zentral gespeichert und für jede US-Behörde und Geheimdienste bequem abrufbar. All das war mir zu keiner Zeit bewusst, als ich vor dem Schalter Stand. Umso größer war meine Ernüchterung, als ich davon erfuhr, was da im Hintergrund so alles gelaufen war. Ich hätte am Procedere auch nichts ändern können, aber gewusst hätte ich ganz gerne, was da auf mich zukommt. Aber diese Erfassungsmethoden sind vergleichsweise harmlos, bedenkt man, was uns in Zukunft erwarten könnte.
Vor einigen Wochen machte eine neue Erfindung Schlagzeilen: Der Nacktscanner. Ein Gerät, das mit Hilfe elektromagnetischer Strahlen ein 3-D-Bild, auf dem der Fluggast ohne Kleidung erscheint, inklusive der Genitalien darstellt. Die EU-Kommission prüft derzeit, ob der Sicherheitsgewinn mittels dieser Geräte den schweren Eingriff in die Privatsphäre der Reisenden rechtfertigt. Unter anderem auch, weil es keine Erkenntnisse darüber gibt, ob die Durchleuchtung für Vielflieger gesundheitliche Folgen haben kann. Derweil werden die Scanner in Zürich, London und Amsterdam bereits eingesetzt.

Nacktscanner-Aufnahmen. Was kommt als nächstes?

WIEVIEL STAAT MUSS SEIN ?

Finden Sie heraus, wie Sie die Überwachungsstaat- Problematik sehen.

Um meine Ergebnisprognose zu sehen, bitte hier Folie 1 auflegen. Sie finden die Folien hinten im Buch.

1. Fragebogen

Diese Umfrage findet im Rahmen einer Bachelor-Thesis an der Fachhochschule Potsdam statt. Die Ergebnisse und Daten werden streng vertraulich behandelt und nicht an Dritte weitergegeben. Es besteht nicht die Möglichkeit, durch die Antworten Rückschlüsse auf einzelne Personen zu ziehen.

1. Wie sicher fühlen Sie sich in Deutschland? Wählen Sie auf einer Skala von 1 – 5, wobei "5" für absolut sicher und "1" für überhaupt nicht sicher steht.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

2. Die Aussage "Ich habe doch nichts zu verbergen, deshalb stören mich staatliche Überwachungsmaßnahmen nicht" trifft für Sie:

- ○ absolut zu
- ○ zum Teil zu
- ○ überhaupt nicht zu
- ○ habe ich noch nie drüber nachgedacht

3. Welche Maßnahmen oder Regelungen sollte der Staat Ihrer Meinung nach verstärkt einsetzen, um die Bürger vor Bedrohungen durch Anschläge und Kriminalität zu schützen?

- ☐ Polizei
- ☐ Verschärfte Sicherheitspolitik
- ☐ Überwachungskameras im öffentlichen Raum
- ☐ Online-Überwachung
- ☐ Abhören von Gesprächen
- ☐ Biometrische Datenerfassung
- ☐ Handy-Ortung
- ☐ Härtere Strafen
- ☐ Verschärfte Ausländerpolitik
- ☐ Sonstiges (Bitte eintragen)

4. Wie wichtig ist Ihnen Ihre Privatsphäre?

- ○ Absolut wichtig
- ○ Wichtig
- ○ Egal
- ○ Nicht so wichtig
- ○ Absolut unwichtig

5. Achten Sie darauf, ob sie von einer Überwachungskamera gefilmt werden?

- ○ ja
- ○ nein
- ○ habe ich noch nie drüber nachgedacht

6. Wenn ja, stört es Sie?

- ○ stört mich immer
- ○ stört mich oft
- ○ ist mir egal
- ○ stört mich selten
- ○ stört mich nie

7. Welche der folgenden Karten besitzen Sie?

- ☐ Kreditkarte
- ☐ EC-Karte
- ☐ Payback-Karte
- ☐ Tankkarte
- ☐ Bahn Card
- ☐ Kundenkarte
- ☐ Sonstige (Bitte eintragen)

Um meine Ergebnisprognose zu sehen, bitte hier Folie 2 auflegen. Sie finden die Folien hinten im Buch.

8. Bewerten Sie die Weitergabe der folgenden Daten an Dritte nach Ihrem Empfinden:

	Ist kein Problem	Unter Umständen	Unter keinen Umständen	Habe ich nie drüber nachgedacht
Name	☐	☐	☐	☐
Anschrift	☐	☐	☐	☐
Geburtsdatum	☐	☐	☐	☐
Familienstand	☐	☐	☐	☐
Private Telefonnummer	☐	☐	☐	☐
Geschäftliche Telefonnummer	☐	☐	☐	☐
Sozialversicherungsnummer	☐	☐	☐	☐
E-Mail-Adresse	☐	☐	☐	☐
Kontoverbindung	☐	☐	☐	☐
Einkommen	☐	☐	☐	☐
Kontostand	☐	☐	☐	☐
Gesundheitszustand	☐	☐	☐	☐
Sexuelle Orientierung	☐	☐	☐	☐
Essgewohnheiten	☐	☐	☐	☐
Einkaufsgewohnheiten	☐	☐	☐	☐
Politische Orientierung	☐	☐	☐	☐
Online-Profile (z.B. Xing/ StudiVZ)	☐	☐	☐	☐

9. Der Verlust welcher der folgenden Dinge (die Rückschlüsse auf Ihre Person zulassen) wäre für Sie besonders unangenehm? Bitte wählen Sie drei Antworten aus und begründen Sie diese kurz. (Wenn Sie eine Begründung schreiben, setzen Sie bitte einen Haken in das Kästchen "Platz für Ihre Begründung")

- ☐ Kreditkarten/ EC-Karten
- ☐ Kontoauszüge
- ☐ Hausschlüssel
- ☐ Autoschlüssel
- ☐ Handy
- ☐ Ausweis
- ☐ Medizinische Rezepte
- ☐ USB-Stick mit Daten
- ☐ Private Fotos
- ☐ Rechnungen
- ☐ Bescheide (z.B.Steuer)
- ☐ Platz für Ihre Begründung

10. Stört es Sie, wenn jemand:

	Stört mich sehr	Stört mich selten	Stört mich nie	Habe ich noch nie drüber nachgedacht
Ihr Gespräch belauscht	☐	☐	☐	☐
Ihr Telefonat mithört	☐	☐	☐	☐
Ihre E-Mails liest	☐	☐	☐	☐
Ihr Handy durchstöbert	☐	☐	☐	☐
Ihre Briefe öffnet	☐	☐	☐	☐
Dateien auf Ihrem Computerbildschirm sieht	☐	☐	☐	☐

Um meine Ergebnisprognose zu sehen, bitte hier Folie 3 auflegen. Sie finden die Folien hinten im Buch.

11. Wie ist es für Sie, persönliche Daten an Unternehmen weiterzugeben?

- ○ Das ist selbstverständlich
- ○ Das ist kein Problem
- ○ Das ist mir unangenehm
- ○ Das möchte ich nicht

12. Geschlecht *

○ männlich ○ weiblich

13. Alter *

14. Berufsgruppe *

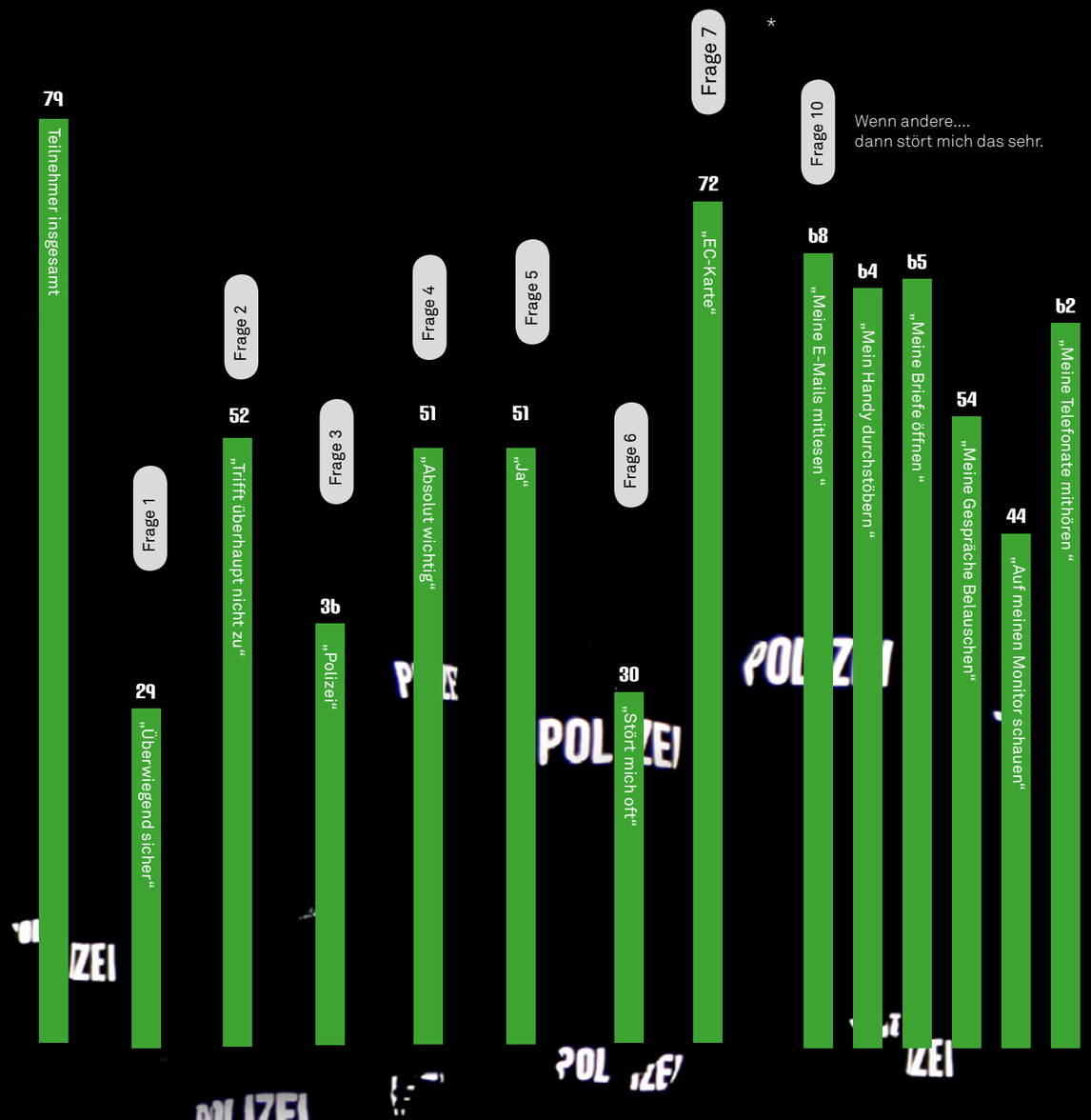
- ○ Arbeitnehmer
- ○ Selbstständiger
- ○ Rentner
- ○ Student
- ○ Schüler/ Azubi
- ○ Arbeitsloser
- ○ Sonstiges (Bitte eintragen)

Erwartungshaltung

Diese Umfrage ist eine Gelegenheit, um herauszufinden, wie sehr der Bürger sich mit seiner Privatsphäre und deren Verletzung beschäftigt. Sie soll herausfinden, ob und wie sich andere mit Überwachung und staatlicher Kontrolle auseinandersetzen, ob sie sie befürworten oder ablehnen.
Die Ergebnisse dienen zum einen der Erkenntnisgewinnung. Sie werden aber auch für spätere Aktionen wie z.B. im Rahmen der „Stick-Attack“ verwendet (Seite 84).
Es wird davon ausgegangen, dass die Beteiligung eher gering ausfällt (80 – 100 Probanden sind das Ziel) da es sich um ein sperriges Thema handelt, über das viele nicht nachdenken wollen.
Außerdem ist anzunehmen, dass jüngere Teilnehmer die staatlichen Maßnahmen mehr kritisieren als ältere. Dafür werden sie mit dem Thema der persönlichen Daten und deren Weitergabe etwas lockerer umgehen. Es könnte sich zeigen, dass Frauen eher ein Verlangen nach „mehr Sicherheit“ haben.
Die Antworten werden insgesamt sehr unterschiedlich sein, sodass es keine eindeutigen Erkenntnisse „für“ oder „wider“ einen Überwachungsstaat gibt.
Der Aufruf zur Teilnahme erfolgte über gezielte Einladungen per E-Mail, über Verteiler und diverse Kommunikationsplattformen. Die eingeladenen Probanden waren aufgefordert, die Umfrage in ihrem Bekanntenkreis weiterzuleiten, um eine möglichst große Streuung zu erreichen. Die eingeladenen Personen wurden bewusst aus verschiedenen Altersklassen, Berufsgruppen und Regionen ausgewählt.

WIEVIEL STAAT MUSS SEIN – DAS ERGEBNIS

Auswerung der Umfrage „Deutschland – Überwachungsstaat?“ (Antwortspitzen)



An der Umfrage beteiligten sich 79 Probanden. (47 Davon männlich, 39 weiblich, 3 machten keine Angaben).
Die meisten Teilnehmer sind Studenten (28) oder Angestellte (21). Der Altersdurchschnitt beträgt 28-32 Jahre. Wenn man sich die Ergebnisse ansieht, entsteht ein eher überraschender Gesamteindruck. Entgegen der Prognose (siehe Seite 51 – 53 in Verbindung mit den Folien hinten im Buch) setzen sich viele Teilnehmer kritisch mit dem Thema Überwachungsstaat auseinander. Das Empfinden für die eigene Privatsphäre ist sehr hoch. Und das Bewusstsein für den Schutz privater Daten stärker als angenommen.
Einige Antworten, vor allem für Frage 8 und 9 waren sogar bestimmend für die weitere Arbeit. (Siehe Seite 84 und 98) Sie wiesen den weiteren Rechercheweg und inspirierten zu einigen Interventions wie den *Mimosa-Stick* oder das *Paranoiker-Handy* (Siehe Seite 89 und 94).

* Die detaillierte Auswertung für Frage 8 und 9 finden Sie auf Seite 86 – 87.

GEDANKEN

Die größte aller Ketzereien war der gesunde Menschenverstand. Und das Furchtbare war nicht, dass sie einen umbrachten, wenn man anders dachte, sondern dass sie vielleicht recht hatten. Denn wie können wir schon wissen, ob zwei und zwei wirklich vier ist? Oder ob das Gesetz der Schwerkraft stimmt? Oder ob die Vergangenheit unveränderlich ist? Wenn beides, Vergangenheit und Außenwelt, nur in der Vorstellung existieren und man die Vorstellung einfach beherrschen kann – was dann?

verbrecher!

Freiheit ist die Freiheit zu sagen, dass zwei und zwei gleich vier ist. *George Orwell, 1984.*

GEWOHNHEITSSACHE

Wo uns Überwachung alltäglich vorkommt.

Google Streetview-Screenshots vom Times Square, New York City.

Fernab von James-Bond- Szenarien und Verschwörungstheorien begegnet uns die vollkommene Überwachung täglich, verpackt in handliche Programme, Services und Technik. In den meisten Fällen da, wo wir sie fast nicht vermuten: Im Supermarkt, auf Downloadportalen, in der Fernsehwerbung oder in Form von harmlosen Add Ons und Applikationen. Diese Applikationen und Services werden es in Zukunft möglich machen, unsere Wege und Gewohnheiten lückenlos zu dokumentieren und nach beliebig vielen Kriterien auszuwerten und letztendlich auch an andere Stellen weiterzuleiten.

Neue Technologien kommen zum Einsatz, um uns das Leben zu erleichtern, oder eben, um uns zu unterhalten.

Über Missbrauch oder damit verbundene Gefahren wird mit Argumenten des erhöhten Komforts für den Kunden oder Nutzer, 100%iger Sicherheit und schwammigen AGBs begegnet. Wer aus Unwissenheit freimütig seine Daten preisgibt, hat im Fall einer Fehlfunktion oder falscher Bedienung immer die Unsicherheit, welcher Schaden ihm persönlich daraus erwachsen kann.

Die folgenden Beispiele zeigen, zu welchen Zwecken man verschiedene Technologien bereits im Alltag einsetzt und welche Gefahren Experten im Zusammenhang mit ihrer Verwendung sehen.

Für Furore sorgte 2007 die Einführung eines neuen Features für Google Maps: *Google Streetview* (Straßenansicht). Fotografierten vorher Satelliten aus dem All die Erde aus der Vogelperspektive und boten diese Bilder in der Kartendatenbank einigermaßen scharf an, waren es nun detaillierte Fotos von anfangs drei Großstädten, die im Netz bewundert werden können. Sie stammen aus Kameras, die auf eine Autoflotte montiert, durch die Städte fuhr und im Sekundentakt Aufnahmen machten. Das ganze ließ sich später im 360° -Blick zusammenmontieren (Siehe Bild). Das Anstößige für Datenschützer hierbei: Dem Betrachter ist es möglich, in die Bilder zu zoomen und zufällig „mitfotografierte" Menschen anzuschauen, die einer Veröffentlichung ihrer Person in diesem Rahmen nicht zustimmen konnten. Da sich zunehmend Protest gegen dieses Google-Spielzeug regt, arbeitet das Unternehmen derzeit daran, abgebildete Personen unkenntlich zu machen. So leiteten private Anwälte in den USA Klagen gegen den Konzern ein, weil ihre Klienten bei Dingen fotografiert wurden, die sie lieber nicht einem riesigen Publikum zugänglich gemacht hätten: Männer, die Strip-Clubs verlassen oder Prostituierte ansprechen, Demonstranten vor einer Abtreibungsklinik,Sonnenbader in Bikinis, Eltern, die ihre Kinder gerade schlugen. [20] Dinge, die isoliert betrachtet, nicht immer dramatisch erscheinen, in der Verbreitung und Vervielfältigung über das Internet aber durchaus unangenehme Konsequenzen mit sich bringen können.

Ein Beispiel für „Überwachungs-Entertainment" sind Applikationen für Handys, mit denen es möglich ist, den Aufenthaltsort bestimmter Personen ausfindig zu machen und metergenau anzuzeigen. Sogenannte *„Friends-Tracker"* sind beliebte Spielzeuge für eifersüchtige Ehemänner und überfürsorgliche Eltern, die mit diesen Methoden massiv in das Privatleben ihrer Angehörigen eingreifen.

In erheblich größerem Umfang kommen verschiedene technische Neuerungen, die auch von Regierungen zur Überwachung und Sicherung des öffentlichen Raumes benutzt werden, derzeit bei der Metro Group zum Einsatz.

Der Konzern betreibt am Niederrhein den ersten „Supermarkt der Zukunft". Im *real,- Future Store* bezahlen bereits jetzt in der Testphase 10% der Kunden, die sich im Rahmen dieses Tests im Vorfeld registriert haben, mit dem Fingerabdruck.[21] Diese Methode soll den Zahlungsvorgang beschleunigen und so das Einkaufen bequemer machen. Der Chaos Computer Club Berlin hat sich eben dieser Datenerfassungsmethode angenommen und in einem dreiminütigen Video schlüssig belegt, wie schnell ein solches Procedere überlistet werden kann. Auch Peter Schaar, Datenschutzbeauftragter der Bundesregierung verweist auf die Gefahr der Fälschung von Fingerabdrücken mit Hilfe von

Mosaik aus Screenshots, die über 365 Tage während Skype-Gesprächen aufgenommen wurden.

„Silikonfingern“. [3]
Ein weiterer Nachteil dieser Systeme ist die korrekte Bedienung. Es wird immer Menschen geben, die ihre Finger nicht richtig auf die Lesegeräte legen und somit Probleme bei der Bezahlung haben werden. Deshalb wird auf Dauer wieder Personal nötig, das den Vorgang überwacht und der Faktor der Zeitersparnis wird sich ebenfalls minimieren.
Andere Unternehmen arbeiten bereits an weiteren Wegen, mit Hilfe von Technik und ohne Personal zu bezahlen:
Eine Alternative zum Zahlen per Finger testet derzeit der Kreditkartenanbieter Mastercard bei einem Lebensmittelhändler im Frankfurter Flughafen. „PayPass“ besteht aus einer Karte, die der Kunde an einem Lesegerät vorbeiführt - schon werden ohne weitere Legitimation Beträge bis zu 25 Euro vom Konto abgebucht. Die Technik lässt sich auch in die Armbanduhr einbauen. „Unsere ersten Erfahrungen zeigen, dass Kunden mit dem System Zeit sparen und mehr kaufen“, sagt Peter Ehmke, Deutschlandchef von Mastercard.
Schon deutlich weiter ist die Branche mit der sogenannten Self-Scanning-Technologie. Kunden führen dabei den Strichcode der Artikel selber am Lesegerät vorbei, bevor sie an der Kasse zahlen. „Nach unseren Umfragen will jeder dritte Händler in Deutschland eine solche Technik zumindest ausprobieren“, sagt Handelsforscher Atzberger. Bei Metro gibt es solche Geräte seit 2003. Im neuen Real-Future-Store in Tönisvorst probiert der Konzern die Technik jetzt erstmals in Verbindung mit dem Handy aus.
Der Kunde fotografiert mit der eingebauten Kamera den Strichcode seiner Waren. Bereits zu Hause kann er per Telefon eine elektronische Einkaufsliste erstellen, indem er den Namen des Artikels eintippt oder den Strichcode von Milch, Joghurt oder Schokolade einliest. Im Laden arbeitet er die Liste ab, und das Handy meldet, was schon im Wagen liegt und was die Produkte kosten. Für die Summe des Einkaufs errechnet das System einen Strichcode, den der Kunde unter ein Lesegerät legt. In der nächsten Entwicklungsstufe soll sogar das Scannen und Abbuchen des Betrages automatisch erfolgen.[21]
Solche Szenarien klingen erstrebenswert, nehmen sie uns doch eine Menge Arbeit ab.

Aber führen solche Versuche nicht auch schnell zu „hirnlosen“ Automatismen?
Ist es wirklich sinnvoll, von Menschen besetzte Arbeitsplätze gegen Systeme einzutauschen?
Neben der Frage nach Datenschutz und Sicherheit, Backup-Systemen bei Versagen der Technik und Schulung im Umgang damit, gibt es einen Punkt, der bei allem Verständnis für neue Wege offen bleibt:
Warum wird in einer Dienstleistungsgesellschaft immer mehr dem Kunden überlassen? Die Antwort darauf liegt auf der Hand. Für Unternehmen, die diese Technik einsetzen, steigen die Umsätze, weil Kunden gezielter „angesprochen“ werden können, Zeit sparen und wegen des entstehenden Komforts mehr kaufen. Weiterhin können Personalkosten reduziert werden. Das ändert aber nicht den Umstand, dass der Einkauf zukünftig vielleicht zum proaktiven Technikabenteuer wird, das nicht jeder bewältigen kann.
Und ein weiterer Fakt sollte nicht außer Acht gelassen werden: Wenn die Akzeptanz für die beschriebenen Szenarien wächst, weil sie einfach eingeführt werden, sinkt damit die Skepsis gegenüber den Gefahren. Und so werden uns an immer neuen Stellen Daten abgeluchst, deren Weiterverarbeitung sich unserer Kontrolle entzieht.
Was kann man aus unseren Einkaufsgewohnheiten ableiten?
Wer kann die Daten der Friends-Tracking-Software oder den Chip in meiner Kreditkarte noch lesen?
Zukünftig wird vielleicht den Ermittlungsbehörden an mancher Stelle die Arbeit erleichtert, weil Informationen über bestimmte Personen ganz einfach im Internet zu finden sind oder durch den Partner oder Supermarkt vielleicht bereits in einem ganz anderen Kontext gesammelt wurden.
Die Mischung aus Unwissenheit, Gutgläubigkeit, Überforderung und Vertrauen in das Tun anderer weicht die Grenzen unserer Privatsphäre zunehmend auf und wird auf Dauer die Hemmschwelle sinken lassen, andere zu bespitzeln, zu beobachten und im schlimmsten Fall vielleicht sogar zu denunzieren.

Diese Bilder stammen aus einer Google-Suche zum Begriff „Kameraüberwachung“. Auf einem Justizblog [22] waren unter einem Artikel, der den aufkommenden Überwachungswahn z.B. via Google kritisierte, duzende Seiten aufgelistet, die Adressen von Sicherheitsdiensten und Technik-Anbietern enthielten, die ihre „Objekte“ frei zugänglich im Netz präsentieren. Ohne Anmeldung oder Passwort gelangt man mit einem Klick in Cafés, Büros, Fußgängerzonen oder observiert langweilige Straßenecken. Es ist möglich, Screenshots zu erstellen. In einigen Fällen gelang es sogar, Details zu vergrößern und die Kamera gezielt zu steuern, bequem mit der Tastatur. Ihren Auftrag, zu schützen nahmen die besagten Firmen, was die abgebildeten Menschen angeht, wohl nicht so ernst. Ob die gefilmten Personen von ihrem Internetauftritt wussten, war nicht herauszufinden.

Die Protokolle sind noch erhalten. Reden über die persönliche Freiheit. Über die persönliche Freiheit untüchtig und unglücklich zu sein. Über die Freiheit, ein kantiger Pflock in einem runden Loch zu sein. *Aldous Huxley, Schöne Neue Welt*

WAS HEISST HIER PRIVAT?

Eine Definition.

Die Privatsphäre einer Person bezeichnet den Bereich, der nicht öffentlich ist, in dem nicht im Auftrag eines Unternehmens, Behörde oder ähnliches gehandelt wird, sondern der nur die eigene Person angeht.

Der Terminus ***Privacy*** wurde 1890 von dem späteren Richter Louis Brandeis und dem Schriftsteller und Rechtsanwalt Samuel Warren im Artikel ***The Right to Privacy*** im Harvard Law Review (Jahrgang 4, Nr. 5) als "Individual's right to be left alone" definiert, also als das Recht eines jeden einzelnen, in Ruhe gelassen zu werden.

Rainer Kuhlen sagt in seinem Buch Die Konsequenzen von Informationsassistenten" auf Seite 417:
„Privacy bedeutet [...] mehr als ‚das Recht in Ruhe gelassen zu werden', sondern das aktive Recht, darüber zu bestimmen, welche Daten über sich [...] von anderen gebraucht werden und welche Daten auf einen selbst einwirken dürfen."

Der Schutz der Privatsphäre ist im deutschen Grundgesetz aus einer Untergruppe des allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 iVm Art. 1 Abs. 1) abzuleiten. Das besondere Persönlichkeitsrecht dient dem Schutz eines abgeschirmten Bereichs persönlicher Entfaltung. Dem Menschen soll dadurch ein räumlicher Bereich verbleiben, in dem er sich frei und ungezwungen verhalten kann, ohne befürchten zu müssen, dass Dritte von seinem Verhalten Kenntnis erlangen oder ihn sogar beobachten bzw. abhören können. Durch die Unverletzlichkeit der Wohnung (Art. 13 GG) und durch das Post- und Fernmeldegeheimnis (Art. 10 GG) wird der Schutzbereich konkretisiert. Die Ausnahmen hiervon (Abhören von Telefongesprächen und Wohnungen) werden als Lauschangriff bezeichnet und sind ebenfalls gesetzlich geregelt.[23]

UND PLÖTZLICH WAR SIE NICHT MEHR DA?

Wie die Auflösung der Privatsphäre über Jahrhunderte den Überwachungsstaat begünstigt.

Als sich das Zusammenleben in einer Gesellschaft noch durch Beziehungen im näheren Umfeld einer Person auszeichnete, war es nicht nötig, persönliche Daten auszutauschen. In den Gemeinschaften kannte und vertraute man sich. Geschäfte wurden per Handschlag besiegelt. Informationen wurden genauso durch das Weitererzählen verbreitet, wie der Ruf einer Person.
In der griechischen Antike gab es erstmals eine Spaltung des Lebens in einen privaten Bereich, der das Haus betraf, und einen öffentlichen, der den Marktplatz einschloss. Öffentlich und damit bekannter als andere, war eine Person aber nur dann, wenn sie sich politisch betätigte. Dies war ausschließlich der oberen Gesellschaftsschicht gestattet.
Die vorindustrielle Gesellschaft in Italien begann, Buch über Leute zu führen, die sich innerhalb von Stadtrepubliks- oder Landesgrenzen aufhielten, mit einem Vermerk, ob es sich bei ihnen um Bettler, Kriminelle oder Handelsreisende dreht. Die Ausstellung von Passierscheinen und Empfehlungsschreiben geschah, damit man die Reisenden jederzeit identifizieren konnte. Man hörte auf, anonym zu sein, unabhängig vom individuellen Status.
Ein bekanntes Überwachungsprinzip, das seit Menschengedenken in die Privatsphäre eindringt, geht von der Kirche aus: Gott sieht alles und er wird dich für deine Sünden bestrafen – ein fester Glaube, der über Jahrhunderte das Verhalten und die Werte der Menschen prägte. Aus Angst, im Fegefeuer zu enden, folgte man den Klerikern und unterwarf sein eigenes Leben ohne jeden Zweifel den göttlichen Gesetzen. Durch Bespitzelung und Druck versuchte man, andersdenkende aus der Gesellschaft zu eliminieren. Ein Klima der Angst vor Folter und brachialen Strafen zwang die Menschen unterdrückt und unwürdig zu leben und im Sinne der herrschenden Klasse handeln. Die Inquisition führte erstmals dazu, dass Listen von Ketzern geführt wurden, um sie bei Wiederholungstaten zu erkennen und die Höchststrafe des Verbrennens bei lebendigem Leib zu vollstrecken. Mit der Zeit wurden Beziehungen vielfältiger und damit unübersichtlicher. Denn sie beschränkten sich nicht mehr auf einen kleinen Kreis von Vertrauten, sondern dehnten sich auch auf flüchtige Kontakte aus, etwa beim Kauf auf einem Markt. Damit nahm die persönliche Bindung stark ab. Man konnte sich nicht mehr sicher sein, wem man vertraute.
Erstmals ergab sich eine wirkliche Notwendigkeit, umfassend Daten über Personen zu erheben. Dies gestattete aber auf der anderen Seite auch, trotz zunehmender Fremdheit und Anonymität, zu planen und zu handeln.
Die Erhebung, Dokumentation und Nutzung von Informationen ist damit eine Voraussetzung für die Herausbildung einer modernen Gesellschaft.[3]
Die industrielle Produktion führte zur verstärkten Aufzeichnung des Alltags:
Buchführung über Prozesse, Arbeitskräfte und Maschinen als Erinnerungshilfe, Beweis- oder Hilfsmittel. Die mündliche Überlieferung reichte für die neuen Anforderungen der modernen Gesellschaft nicht mehr aus. Deshalb wurde die Verarbeitung von Daten selbst ebenfalls Maschinen übertragen.
Dieser Schritt führte letztendlich dazu, dass die Massendatenverarbeitung erstmals im Staatsdienst 1890/91 mit einer Volkszählung in den USA begann.

Während Regime die Macht über Deutschland hatten, kam es zur umfassendsten Datenerhebung in der Geschichte. Die Privatsphäre der Bürger wurde durch staatliche Maßnahmen vollkommen aufgehoben. Kontrolle, Bespitzelung und der Zwang zur absoluten Offenlegung aller persönlichen Verhältnisse waren charakteristisch für zwei vollkommen gegensätzliche politische Strömungen. Der Verlust der persönlichen Freiheit, Grausamkeit und Mord traurige Resultate zweifelhafter Staatsmächte. Das Leid das damit verbunden war, ist bis heute nicht vergessen.

Gott sieht alles – aber er petzt nicht!

Durch die ständige Weiterentwicklung der Maschinen bis hin zum PC und der Erfindung des Internet, beschleunigte sich auch die Auflösung der Privatsphäre und damit die Chance der fortschreitenden Erfassung und Verbreitung von immer mehr Informationen über Personen.
Die Presse oder besser, die neuen Massenmedien tragen in der heutigen Zeit erschwerend dazu bei, dass der Begriff Privatsphäre sehr dehnbar geworden ist.
Immer persönlicher werden die Geschichten, immer pikanter die Details. Alles für die Auflage. Das Eindringen in jeden Bereich des Lebens– vor allem von Prominenten, möglichst großformatig auf Fotos dokumentiert, verwässert die Grenze zwischen privatem und öffentlichem Leben zusätzlich. Und es führt dazu, dass nicht öffentliche Personen einen sehr verschobenen Begriff der Privatsphäre anderer serviert bekommen. Es scheint fast so, als wäre ihre Bedeutung einigen bereits nicht mehr bewusst. Vergegenwärtigt man sich dann noch die peinlichen Veröffentlichungen vieler Zeitgenossen auf diversen Internet-Communities, wird dieser Eindruck nur abgerundet.
Das Ende der Privatsphäre kommt nicht plötzlich und erst recht nicht allein durch die Hand des Staates.
Doch ihre langsame Auflösung, an der wir uns zuweilen aktiv beteiligen, wird dazu führen, dass wir bald unfreiwillig Dinge von uns preisgeben müssen, die, wenn sie in falsche Hände geraten sogar gegen uns verwendet werden könnten.
Immer neue Technologien werden einen Platz in unserem Leben finden, um es für uns „sicherer“ und für andere kontrollierbarer zu machen.
Wenn wir unsere Privatsphäre nicht selbst ein bisschen im Auge behalten, wird es bald keinen Raum mehr geben, für unsere persönliche Freiheit.

[SOCIAL] COMMUNITIES

Was ist der Preis für ihre kostenlose Nutzung?

Als das Internet anfing, den Kinderschuhen zu entwachsen, hatten viele Firmen Interesse daran, mit dem neuen Medium Geld zu verdienen. Unzählige webbasierte Unternehmen schossen wie Pilze aus dem Boden. Das Geschäft fand vor allem an den Börsen statt, bis es zum Zusammenbruch kam: Nachdem Ende 2001 die große Internet-Blase geplatzt war, hielt man das Internet für einen überschätzten Hype. Vor allem die Kapitalgeber und Firmen zogen sich zurück. Kein Wunder, haben sie doch dabei viel Geld verloren. Tatsächlich ist es - zumindest in Deutschland - nach wie vor so gut wie unmöglich Kapital für die Gründung eines Internet-basierten Unternehmens zu erhalten.[25]

Die kommerzielle Ebene der Webnutzung beschränkte sich zunächst auf Versteigerungs- und Einkaufsdienste. Neben diesem Zweig entstand aber auch ein ganz neues Nutzungsprinzip, das seinen Namen von Tim O´Reilly* bekam: Web2.0.

Es ist gekennzeichnet durch interaktive und kollaborative Elemente, die für den Nutzer einen persönlichen Mehrwert generieren. Begriffe, die im Zusammenhang mit dieser Entwicklung stehen sind vor allem User Generated Content (Nutzergenerierte Inhalte), Geotagging (Zuweisung raumbezogener Referenzinformationen zu einem Datensatz), Crowdsourcing (Auslagerung von Unternehmensaufgaben auf die Intelligenz und die Arbeitskraft einer Masse von Freizeitarbeitern im Internet), Feed (Transportmechanismus für Informationen z.B. aus Foren, abonnierbar), Citizen Journalism (Bürger-Journalismus) und Social Networking (Soziales Netzwerken). Letzteres geschieht vor allem über Online-Communities – Netzwerkgemeinschaften, die Plattformen zum Veröffentlichen und Austauschen verschiedenster Inhalte besuchen. Nutzer dieser Plattformen entblößen sich durch die Angabe vieler privater Daten und Interessen öffentlich und bieten damit auch ein interessantes Ziel für Staatsgewalt und Wirtschaft. Erstere kann, ohne ein eigenes Netzwerk bemühen zu müssen, nahezu jede Information zum angemeldeten Benutzer, sollte der in irgendeinem Zusammenhang unter Verdacht geraten, bekommen – neuerdings sogar ganz einfach direkt vom Betreiber. (Siehe Seite 74).

Die Communitybetreiber machen sich darüber hinaus zusammen mit der übrigen Wirtschaft langsam von neuem auf den Weg, im Web Geld zu verdienen – mit den Daten der Web2.0-Nutzer.

Google hat als einziges Unternehmen den Crash überlebt. Ein riesenhaftes Netzwerk macht seit Jahren ein millionenschweres Geschäft möglich: Man verdient Geld, indem man uneingeladen und unsichtbar in die Privatsphäre seiner Nutzer eindringt, Mails mitliest und Webseiten scannt, um mit Hilfe der generierten Daten keyword-basiert Werbung zu schalten. Die Währung dafür heißt Klicks und Page-Impressions. Der Börsenwert von Google beruht zum Großteil auf der Hortung von Informationen und der Technologie für effizientes Durchsuchen von Inhalten. Unter dem Firmen-Motto „Do no evil“ (Tu nichts Böses) wird also mit gezielter Online-Spionage die Kasse zum Klingeln gebracht. Ein Web 2.0-Konzept, das viele Firmen nur zu gern kopieren würden.

Google und Communities bilden außerdem die Werkzeuge für einen weiteren Trend.

Es ist immer selbstverständlicher für Arbeitgeber, Bewerber im Vorfeld zu „googeln“, um sich einen Eindruck abseits des persönlichen Gespräches zu verschaffen. Communities sind die Lebensläufe des Web 2.0 und unsere Privatsphäre ist für jedermann öffentlich zugänglich geworden. Immer wieder gibt es Probleme mit Chefs, die die privaten Interessen und Vorlieben ihrer Mitarbeiter online überwachen und bei Missbilligung auch Konsequenzen ziehen (Siehe Seite 81).

** Tim O'Reilly (* 1954 in Cork, Irland) ist Gründer und Chef des O'Reilly Verlages, sehr aktiver Softwareentwickler im Bereich freier Software und maßgeblich an der Entwicklung der Skriptsprache Perl beteiligt. Er ist Autor mehrerer Bücher, die er in seinem eigenen Verlag vertreibt. Mit seinem Artikel über das Web 2.0 trug er maßgeblich zur Durchsetzung und einheitlichen Wahrnehmung dieses veränderten Internet-Musters bei. O'Reilly Media veröffentlichte 1992, als es nur wenige hundert Webseiten im ganzen Netz gab, das erste Buch im Internet. O'Reilly Media erschuf 1993 ebenso das erste Web-Portal, den Global Network Navigator, kurz GNN. Diese Seite, die als erste überhaupt Werbung schaltete, wurde 1995 an AOL verkauft.* [26]

[SOCIAL] COMMUNITIES IM ÜBERBLICK

Einfach anmelden , einloggen und mitmachen.

Web 2.0

Web 1.0

studiVZ ★
myspace.com ★
facebook
meinVZ ★
schülerVZ ★
StayFriends ★
Ning

YouTube ★
MyVideo ★
CLIPFISH
sevenload
vimeo
flickr ★
photocase ★
fotocommunity ★
VIEW
last.fm ★

Slashdot
YIGG
Technorati

XING ★
LinkedIn
monster ★

delicious ★
digg
furl
reddit
oneview

yasni.de

Google ★
YAHOO! GROUPS ★

THE WELL
AOL
YAHOO! GeoCities

skype ★
twitter
iChat
msn

Klassische Online-Communities zum Erstellen eines Nutzerprofils, das für andere sichtbar gemacht werden kann. Verknüpfung von Daten Interessen, Freunden und Fotos zu einer Person. Erleichtet das Suchen angemeldeter Personen nach verschiedenen Kriterien.

Plattformen zum Hochladen, Veröffentlichen, Bewerten, Austausch und Download von eigenem Foto- und Videomaterial. **LastFM** eignet sich zum Finden Bewerten und kostenlosen Hören von Musik. Es speichert den Musikgeschmack des Nutzers und richtet eine angepasste Bibliothek ein.

Blogs zur Erstellung, Weitergabe und Verbreitung von Nachrichten. Erstellte Inhalte können jederzeit und weltweit dem Verfasser zugeordnet werden.

Die professionelle Version der Online-Communities. Zum Finden von Geschäftspartnern und Auftraggebern. Zum Versenden von Einladungen zu Firmenevents. Kontaktplattform für Angestellte und Geschäftsführer. Bewerberplattform. Erstellung eines detaillierten Jobprofils.

Social Bookmarking. Archivierung , Speicherung und Weitergabe von Webinhalten auf Basis persönlicher Interessen der Benutzer. Empfehlungsprinzip.

Ein Suchdienst, der im gesamten Web eingestellte Informationen und Bilder zur eingegebenen Person aufspürt und darstellt. Die Detailsuche ist anhand beliebiger Kriterien (Anschrift, E-Mail) möglich. Es kann ein genaues Personenprofil generiert werden.

Ermöglichen das Sammeln und Archivieren von Artikeln aus Information- und Diskussionsforen. Stammen aus der Zeit, bevor soziale Netzwerke im Internet beliebt wurden.
Sie bringen Nutzer anhand bestimmter Interessen zu (Diskussions-) Gruppen zusammen.

Diese mit einem schwarzen Brett vergleichbaren Dienste kann man als Vorreiter der heutigen Online-Communities bewerten. Vornehmlich Diskussionsplattformen. Kostenloses Erstellen und Hosten einer eigenen Website bei **Yahoo GeoCities** möglich.

Social Software/ Plattformen, mit deren Hilfe der Nutzer weltweit via Textnachrichten (Chat) oder Videotelefonie mit seinen „Freunden“ online verbunden ist. **Twitter** veröffentlicht dabei minutengenau, was der Nutzer im Augenblick tut. In Skype geschieht dies über die Moodmessages.

Legende

☠	Im Zuge der Recherche negativ aufgefallen im Umgang mit Daten und Nutzerprofilen (Weitergabe an Dritte, Überwachung)
★	In Deutschland sehr beliebte Plattform.
$	Monetäres Interesse. Äußert sich u.a. in Gebührenerhebung oder das Anbieten von Nutzerdaten an die Wirtschaft für z.B gezielte Werbeschaltung.

ARE YOU READY FOR A NEW HIT?

StudiVZ, Ermittlungserfolge und die Wirtschaft.

Als StudiVZ 2005 online ging, war es vom Erfinder Ehssan Dariani als Social Network geplant. Austausch für Studenten. Inzwischen wurde einiges ausgetauscht. Rechte, Besitzer, eine Menge Geld, die AGB und im Hintergrund auch das Konzept.
Als die Plattform anfing zu wachsen, kamen Investoren wie Lukasz Gadowski und Matthias Spiess, Gründer von Spreadshirt (Stasi 2.0-Shirt-Unterstützer, siehe Seite 36). Später wurde StudiVZ vor allem durch die Gebrüder Samwer („Jamba“) finanziert. Heute ist der Holtzbrinck Verlag („Die Zeit“, „Handelsblatt“) Besitzer. Derzeit haben die Plattformen studiVZ.net, schuelerVZ.net und meinVZ.net nach eigenen Angaben mehr als 10 Millionen Nutzer. (Quelle Spiegel online) Damit wurde eine studentische Idee, klug abgekupfert vom amerikanischen Vorbild „Facebook“, innerhalb von nur 2,5 Jahren Gegenstand massiven Interesses großer Wirtschaftsunternehmen. Diese erkannten schnell das ungeheure Potenzial der Plattform: Eine freiwillige Sammeldatei deutscher Studenten, eine Informationsfundgrube, ein Interessenprofilgenerator.
Versuche der Rechteinhaber, mit den Profilen der Nutzer Geld zu verdienen, zeigen ersten Erfolg:

Im Dezember sorgte der Plan von StudiVZ für Aufregung, Nutzern personalisierte Werbung auf Basis der persönlichen Informationen aus den Mitgliederprofilen zu präsentieren. StudiVZ änderte dafür die Geschäftsbedingungen. Wer nicht zustimmte, sollte rausfliegen. Experten zweifelten daran, dass die Methode gesetzeskonform ist. Die Verbraucherzentrale Bundesverband mahnte StudiVZ im Februar ab – mehr als 90 Prozent der StudiVZ-Mitglieder haben der Nutzung ihrer Profile für personalisierte Werbung schon zugestimmt - mit einem Mausklick. [27]

Auch ich habe den neuen Nutzungsbedingungen zugestimmt, nachdem ich sie sorgfältig gelesen hatte – das erste Mal in meinem Leben.
Danach war ich auch nicht schlauer. Die vier Seiten klangen eigentlich harmlos. Für mich ging nicht eindeutig daraus hervor, was genau jetzt neu ist im Umgang mit meinem Profil, meinen Daten. Die Verfasser wurden in persönlich an mich adressierten Mails nicht müde zu beteuern, dass sich für mich und mein Profil nichts ändern würde, dass keine Daten an die Wirtschaft verkauft werden würden oder ich sonstiges zu befürchten hätte.

Das einzige, das eindeutig wurde, war die Tatsache, dass man mich leider exmatrikulieren müsse, wenn ich nicht bereit wäre, den neuen AGBs zuzustimmen.
Heute sieht das ganze folgendermaßen aus: Ich bekomme wann immer ich mich ein- oder auslogge von genau vier Anbietern immer die gleiche Werbung auf meine VZ-Seite geschossen. Auf zwei der beworbenen Seiten bewege ich mich ohnehin regelmäßig, bin ich sogar angemeldet. Das führt bei mir dazu, dass ich die Banner überhaupt nicht mehr wahrnehme. So gesehen habe ich mir mit meiner Zustimmung die Chance darauf vergeben, wie vorher, durch irgendeine Werbung vielleicht zufällig etwas Neues kennenzulernen.
Die Befürchtung, die Herr Riecke (GF StudiVZ, früher u.a. bei Bertelsmann, AOL, Lycos und Ebay) im Spiegel Online Interview zur Rechtfertigung der gezielten Werbung äußert, macht mir also keine Kopfschmerzen:

SPIEGEL ONLINE: Werbekunden können derzeit nach Alter, Geschlecht, Wohnort und Studienrichtung sortieren. Was kommt als nächstes?
Riecke: Da haben wir keine konkreten Pläne. Diese vier Kriterien sind den Wer-

bekunden am wichtigsten. Wir müssen das erst sauber umsetzen, die Reaktionen prüfen. Nichts wäre schlimmer als Beschwerden der Nutzer, dass sie nun irrelevante Werbung bekommen. Laut unseren Umfragen akzeptiert die Mehrheit der Nutzer personalisierte Werbung eher als irrelevante. Die wird als Spam wahrgenommen. (...) Die Marktforschung zeigt klar, dass personalisierte Werbung besser akzeptiert wird. Deshalb wollen wir auch die zehn Prozent unserer Nutzer, die noch nicht zugestimmt haben, davon überzeugen. Es geht uns hier nicht um das Werbegeld. Ich denke, wir werden die Nutzer eher verlieren, wenn sie sich über irrelevante Werbung ärgern."

Bis zum Zeitpunkt der Recherche für diese Arbeit war mir nicht bekannt, welche Daten genau an die Werbetreibenden ausgegeben werden. Bis heute ist nicht in Erfahrung zu bringen, in welchem Umfang und an welche Unternehmen dies geschieht.
Das ist nicht das einzige, was aus den AGBs denen ich vor ca. 8 Monaten zugestimmt habe (inzwischen wurden sie sicher einige Male „angepasst"), nicht hervorging. Im Spiegel Online Interview offenbart Herr Riecke eine weitere Überraschung:

SPIEGEL ONLINE: Lassen sie nicht Text- und Bildscanner über das Angebot laufen?
Riecke: Ja, aber die sind zu unzuverlässig.

Es gibt aktuell leiden keine technisch ausgereiften Lösungen. Allein auf Basis dieser Treffer können wir nicht handeln. Wir filtern nicht automatisch Dateien, die hochgeladen werden. Wir machen, wozu wir gesetzlich verpflichtet sind: Bei nachgewiesenem Kenntnisstand müssen wir innerhalb der Frist des Telemediengesetzes reagieren. Das tun wir.
Das bedeutet im Klartext, StudiVZ scannt selbst Inhalte der Plattform. Sollte ein „Treffer", d.h. ein gesetzeswidriger Inhalt einmal Gegenstand einer Ermittlung durch die Polizei oder das BKA werden, ist das VZ dazu verpflichtet, konkrete Inhalte der betroffenen Profile weiterzugeben.
An einigen Stellen ist das ganz im Sinne vieler Nutzer, die sich mehr Kontrolle wünschen: Während die Mitgliederzahl rasant wuchs, kam StudiVZ nicht immer mit der Kontrolle der Inhalte hinterher. Betroffene warfen StudiVZ vor, zu wenig gegen die organisierte Belästigung von weiblichen Mitgliedern und antisemitische, links- sowie rechtsextreme Propaganda vorzugehen. [27]
Aber mit Hilfe dieser Methode finden Bundesbehörden, Ministerien und Justiz zunehmend Zugang zu dieser Community und damit Wege, ohne eigenes Zutun an Benutzerdaten zu gelangen. Mit Hilfe des VZ können sie Deutschlands Studenten genau unter die Lupe zu nehmen. Laut Riecke werden etwa 10 mal die Woche konkrete Anfragen von Behörden an StudiVZ gestellt.
Am häufigsten zum Thema Jugendschutz, Beleidigung, Volksverhetzung, Verletzungen von Persönlichkeitsrecht zum Beispiel durch Fake-Profile.
Das mag man für die ersten drei Punkte einsehen, denn davon nimmt jeder vernünftige Mensch Abstand. Aber allein das Ändern oder Abkürzen des Namens stellt laut Definition die Einrichtung eines Fake-Profils dar. Mache ich mich selbst damit bereits strafbar? Sollte die Polizei mein Profil bei StudiVZ einmal rein „interessehalber" besuchen, wahrscheinlich schon.
Sollte sie dann auch noch Anfragen, in welchem Zusammenhang oder zu welchem konkreten Gegenstand auch immer: StudiVZ wird meine Daten mit meiner Erlaubnis weitergeben, sollte Herr Riecke seine Aussage ernst meinen:

„Wir stehen da zwischen den Fronten. Auf der einen Seite der Datenschutz, auf der anderen Seite die Ermittler. Das Telemediengesetz verbietet uns, ohne Zustimmung der Nutzer Nutzungsdaten zu speichern. So hat der BGH vorigen Herbst entschieden. Die Kripo- und LKA-Beamten verlangen aber genau diese Daten von uns, die wir laut Datenschützern nicht speichern dürfen. Deshalb haben wir die Nutzer der Speicherung der Nutzungsda-

ten zustimmen lassen. (...) Gott sei Dank dürfen wir bei Ermittlungsersuchen solche Daten nun herausgeben. Nutzungsdaten speichern wir bei allen Nutzern, die uns das erlaubt haben durch ihre Einwilligung.“
Gott sei Dank habe ich dem zugestimmt! Dumm nur, dass mir das zu keiner Zeit in den AGBs in dieser Form vorlag. Denn ich sollte mich nur entscheiden, ob ich personalisiert beworben, oder exmatrikuliert werden will. Die Aussage Rieckes zur Weitergabe von Nutzerdaten hat große Empörung ausgelöst. Später dementierte er und gab an, Spiegel Online hätte ein verkürztes Zitat verwendet, das den Sinn seiner Worte verzerre.
Das systematische Ausspionieren von StudiVZ-Inhalten steckt aber noch in den Anfängen und es ist nicht klar, ob Ermittlungsbehörden eigene Mittel verwenden, um an gewünschte Inhalte zu kommen. Glaubt man der Aussage des Betreibers einer Webseite, auf der StudiVZ-Profildaten nach verschiedenen Faktoren ausgewertet vorliegen, war das früher ganz einfach:
Um einen möglichst konsistenten Zustand der ausgelesen Daten zu erhalten, war es von Bedeutung in möglichst kurzer Zeit alle Profile auszulesen. Durch die Verteilung der Clients in ein Rechner-Cluster aus 10 Maschinen gelang dies innerhalb von weniger als vier Stunden. StudiVZ hat einige Maßnahmen eingeführt, um das automatisierte crawlen der Profile effektiv zu verhindern. Ein „Abgrasen“ ist demnach nur noch in sehr begrenztem Maße mit hohem Zeit- und Arbeitsaufwand möglich. Mir ist nicht bekannt, dass seit Dezember 2006 neue Versuche unternommen wurden.[28]
Um dieses Abgrasen in Zukunft effizienter zu praktizieren, hat der VZ-Betreiber bereits eigene Vorschläge, die aber nicht er, sondern ganz andere Stellen in Zusammenarbeit umsetzen und anwenden sollen. Zum Beispiel zum Schutz vor der Verbreitung von jugendgefährdenden Inhalten vor allem auf Schüler VZ. Oder die Bedrohung durch Pädophile, die mit Fakeprofilen arbeiten. Riecke auf die Frage, ob man sich nicht auch unter Vortäuschung falscher Tatsachen Zugang zu Profilen junger Nutzer erschleichen könne: **„Ja, klar, man kann sich anmelden und die AGB verletzen. Es gibt derzeit kein Altersverifizierungssystem für Jugendliche unter 16. Das können wir auch nicht allein aufbauen. Da müssen sich die Ministerien, Behörden und großen Unternehmen auf dem Feld zusammensetzen. Da gibt es auch zwischen den verschiedenen staatlichen Stellen zu wenig Koordination. Warum müssen wir etwa die AGB ändern, um Ermittlern die verlangten Auskünfte geben zu können?“** Die Motive für eine Zusammenarbeit gegen die genannte Gefahr sind verständlich. Aber die Nutzung der erhobenen Daten zu anderen Zwecken steht ebenso bedrohlich im Raum.

Wir haben die Geschäftsbedingungen und die Datenschutzerklärung aus zwei Gründen geändert. Zum einen, um zielgerichtet werben zu können. Zum anderen, um Konflikte mit Ermittlungsbehörden zu vermeiden.

Marcus Riecke, CEO von StudiVZ

Die geringste Kleinigkeit konnte einen verraten. Ein nervöses Zusammenzucken, ein unbewusster Angstblick, die Gewohnheit, vor sich hinzumurmeln – alles, was den Verdacht des Ungewöhnlichen erwecken konnte, oder dass man etwas zu verbergen habe. Einen unpassenden Ausdruck im Gesicht zu zeigen […] war jedenfalls schon an sich ein strafbares Vergehen.

George Orwell, 1984.

WAS IS´N DABEI?

Warum es manchmal besser wäre, nicht zu viel von sich zu veröffentlichen.

In den letzten Wochen sind diverse Skandale im Zusammenhang mit Kundendaten durch die Presse gegangen. Bei Banken, Kreditkartenfirmen, Behörden und Telekomunikationsanbietern war von „Datenpannen" die Rede. Pannen, bei denen Zugangsdaten und persönliche Informationen von Privatpersonen entweder gestohlen, versehentlich veröffentlicht oder falsch versendet wurden, in millionenfacher Höhe. Ebenso war immer wieder zu hören, dass sogenannte Datenlöschdienste ihre Arbeit nur wenig ernst nahmen und Festplatten aus Regierungskreisen auf dem Flohmarkt verkauften, wo Käufer mit wenig Anstrengungen alle Inhalte wieder herstellen konnten.

Auch der gezielte Austausch und Verkauf von Datensätzen taucht im Rahmen dieser Skandale am Rand auf. Nun hat man bei den genannten Stellen meist keine Möglichkeit, sich der Angabe gewisser persönlicher Daten zu entziehen, erst Recht gibt es keine Kontrolle darüber, was mit ihnen im weiteren Verlauf der Bearbeitung geschieht. Aber diese Skandale nur hinzunehmen, reicht wohl auch nicht aus. Für diese Fälle hat es in Zukunft Regelungen zu geben, Gesetze, etwas das wir alle gemeinsam fordern sollten. Unsere Daten sind nicht fiktive Binärcodes aus einer fremden Welt. Sie verschlüsseln unsere Identität. Die folgenden Beispiele zeigen, was passieren kann, wenn man diesen Fakt leichtfertig unterschätzt.

Schnüffelwirtschaft:

Auf den wachsenden Zugriff auf Community-Profile durch Ermittlungsbehörden wurde bereits eingegangen. Während der Recherche tauchte aber ein weiterer interessanter Fall der „präventiven Kontrolle" auf. In einer BDU-Umfrage (Bundesverband Deutscher Unternehmensberater) gab jeder Dritte der Befragten Geschäftsführer an, Onlineprofile von Bewerbern anzusehen, bevor er ihn zum persönlichen Gespräch einlädt. Einige nutzen die Online-Reputation als Ausschlusskriterium. Tatsächlich wird es dank Google immer selbstverständlicher, sich einen Eindruck über Personen zu verschaffen, ohne dass diese etwas davon mitbekommen. Was früher im persönlichen Gespräch geschah, ist heute für niemanden mehr zu beeinflussen. Den ersten Eindruck hinterlässt man digital. Deshalb ist es zunehmend wichtig darauf zu achten, was man im Netz über sich zugänglich macht.

Die Generation, die mit Youtube, Myspace und Co groß geworden ist, wird dies in Zukunft zu spüren bekommen. Partyexzess-Videos, peinliche Fotos und dämliche Kommentare stehen nicht im Lebenslauf –aber auf Personensuchmaschinen.

Das kann dem wahren Image erheblich schaden, gibt es genug Angriffsfläche für Missinterpretation. Mit dem Bekanntwerden einiger „personeller Konsequenzen" aufgrund vermeintlich kompromittierender Webinhalte, ist ein neuer Trend zu verzeichnen. Es existieren bereits spezielle Angebote die das digitale Image etwas aufpolieren. Sogenannte Reputation Defender (Rufschützer) werden zukünftig wohl gute Umsätze zu verzeichnen haben, denn diesen Dienst muss man selbstverständlich bezahlen. Communities sind weitgehendkostenlos (Siehe Community-Übersicht, Seite 72), solange man sie nicht als Plattform für kannibalisierende Selbstdarstellung sieht.

Wer ein wenig auf sein Profil achtet, kann den Umstand, dass zukünftige Arbeitgeber sich gern mal einen ersten Eindruck verschaffen, sogar als Sprungbrett nutzen.[29]

Unsere Online-Reputation sollten wir genauso im Auge behalten, wie unsere reale. Wer zu viel über sich veröffentlicht, oder

veröffentlichen lässt, steht schnell ohne Privatsphäre da. Das Internet ist für viele ein Versprechen für schnellen Ruhm und Prominenz. Aber es wird auch zunehmend ein Instrument, um Druck auf Personen auszuüben und sie öffentlich bloßzustellen. Der Wahnsinn kennt dabei keine Grenzen. In Korea erschütterten im Oktober 2008 zwei Selbstmorde das „bestverkabeltste Land der Welt“ Eine beliebte Schauspielerin und ein Model, das sich in einer Fernsehshow outete, mussten im Netz üble Verleumdungen, Beschimpfungen und Drohungen über sich ergehen lassen. Sie sind zwei der sechs bekanntgewordenen prominenten Opfer, die von einem Online-Lynchmob während der letzten 2 Jahre in den Tod getrieben wurden. Als im Mai 2008 mehr als 80.000 Menschen bei dem großen Erdbeben in Zentralchina starben, wurden die Toten online von den Koreanern verhöhnt.[30]

Dies ist die Kehrseite einer Gesellschaft, die sich im Zeitalter der Internetdemokratie angekommen glaubte, in der ein offener Online-Diskurs für alle herrsche.

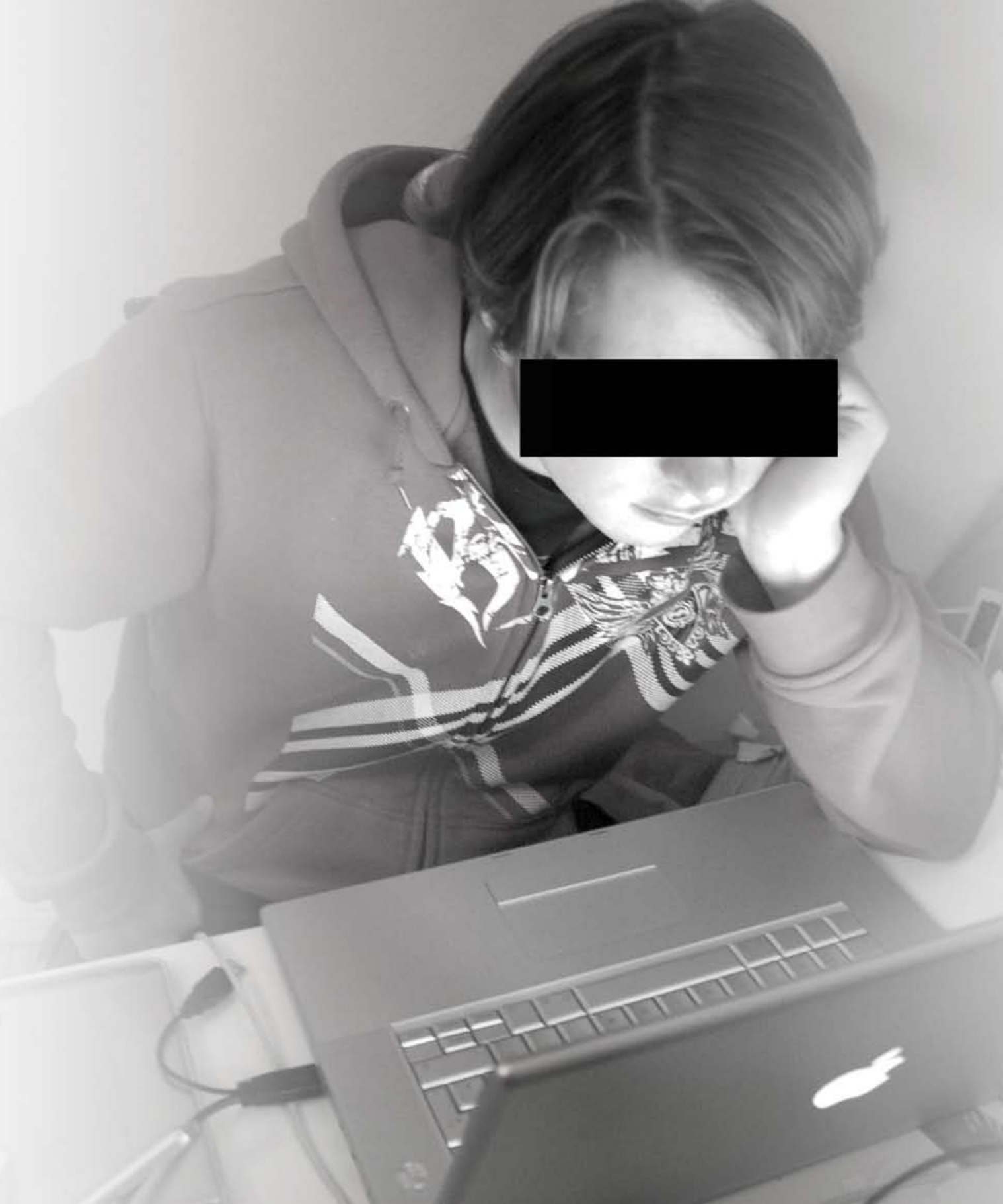
Die sonst so um die Wahrung ihres Gesichtes bemühten Koreaner lassen im Netz die Sau raus: Im Schutz vermeintlicher Anonymität verwandeln sich Kinder, Hausfrauen und Büromenschen in Stalker, Gerüchteerfinder und Rufmörder. Aus Neid, Frust und Langeweile wird Cyberterror. Aus dem demokratischsten aller Medien wird ein Folterinstrument.[30] Die Regierung will jetzt gegen die virtuelle Hexenjagd vorgehen. Mit einer Internetpolizei. Anonymität soll es nicht mehr geben. Wer zukünftig im Netz beleidigt, muss mit Strafen rechnen. Experten befürchten eine Zensur des Internet, wie in China. An den Schulen überlegt man, als Präventivmaßnahme „Cyberkultur“ oder „Netiquette“ einzuführen.

Das Land, das im Ranking der Länder, die um den Schutz der Daten ihrer Einwohner bemüht sind, auf einem der hinteren Plätze rangiert, geht noch einen Schritt weiter :

In Amerika veröffentlichte die Polizei eine Liste verurteilter Täter, die sich des Kindesmissbrauchs strafbar gemacht hatten, nebst Adresse im Internet. Einige der Männer von dieser Liste kamen durch die Hand eines wütenden Mob aufgebrachter Bürger um, nachdem sie ihre Strafe abgebüßt hatten.[3] Dieses Beispiel zeigt besonders dramatisch, wozu „Pannen“ und Fehler führen können. Solche Fälle zu verhindern ist wohl die größte Herausforderung, die uns bei der Weiterentwicklung des Internet und der Informationsgesellschaft bevorstehen. Transparenz, Mitwirkungsmöglichkeiten und Datenschutz sollten zukünftig die bestimmenden Grundpfeiler sein.

Die beschriebenen Beispiele sind Einzelfälle. Können sie dazu führen, dass eine staatliche Überwachung und Kontrolle des Internet vollkommen legitim wird? Werden wir zukünftig nicht mehr einfach so unsere Gedanken, Fotos oder Filme tauschen können, aus Angst jemand könnte daran Anstoß nehmen und Konsequenzen ziehen?

Es muss eindeutige Regelungen für das Internet geben, damit nicht alle Nutzer ständig unter Generalverdacht stehen. Dazu muss jeder die Chance erhalten, mehr Kontrolle über seiner veröffentlichten Inhalte zu haben. Um gezielt kriminelle Handlungen herauszufiltern, müssen sich Experten und Behörden enger abstimmen und das Netz wirklich verstehen lernen, damit es aufhört, in den Augen der älteren (Politiker-) Generation ein böses Buch mit sieben Siegeln für Schurkereien und Abzocke zu sein. Wenn einige wenige kontrollieren, was wir online machen und an zu vielen Stellen eingreifen, um zu bestimmen, was richtig oder falsch ist, wäre dann nicht auch der demokratische, freiheitliche Grundgedanke des Web in Gefahr?



Stick Attack.

Sind Dateien Gegenstand unserer Privatsphäre?

Wenn man einen Stick mit persönlichen Dateien verliert, ist das irgendwie ärgerlich. Oftmals finden sich Dinge darauf, die ohnehin noch irgendwo anders gespeichert sind. Und eigentlich war das Zeug darauf auch gar nicht so wichtig. Meistens ist das so. Trotzdem beherbergen die kleinen Speicher Informationen über ihren Besitzer. Im schlimmsten Fall ist sogar das einzige Back-Up der aktuellen Version einer wichtigen Arbeit darauf zu finden. Oder das Angebot der Versicherung, das gestern per Mail reinkam und das bis zum Ausdruck dort zwischengelagert wurde. Oder auch die Scans der Kontoauszüge, die nachher noch schnell zum BaföG-Amt geschickt werden sollten, damit der Antrag endlich vollständig ist.

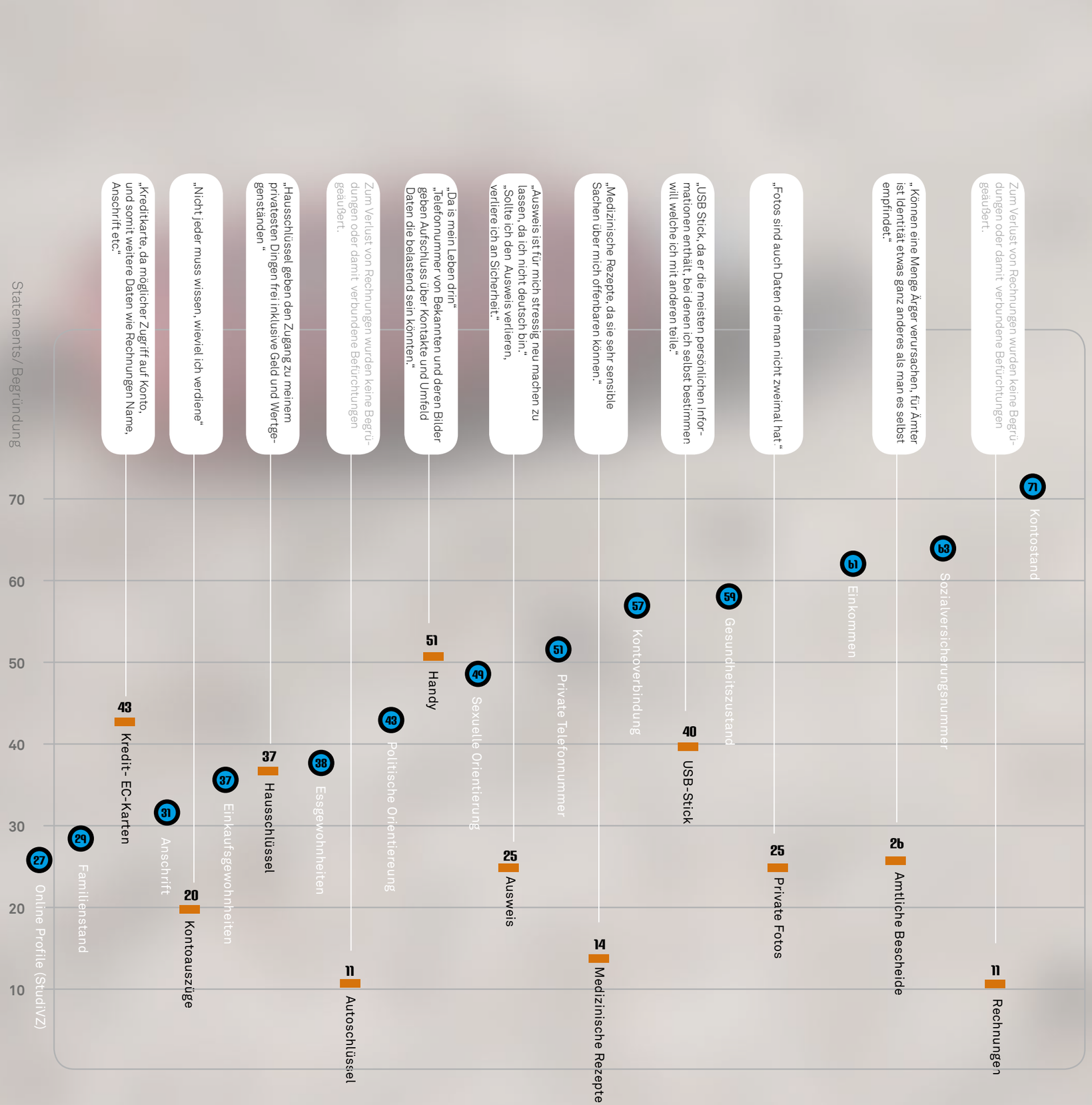
Wenn man einen Stick verliert, fängt man an, nachzudenken, was man da eigentlich verloren hat. Peinliche Fotos? Wichtige Dokumente? Unwichtigen Schrott?

Was kann der Finder damit anfangen? Wird er sich die Daten anschauen, sich einen Eindruck vom Besitzer verschaffen? Wird er die Wichtigkeit des Inhaltes prüfen und sich dann, findest er einen Kontakt irgendwie melden? Oder ist dieser Stick nur ein billiges Spielzeug, das man löschen und selbst behalten kann?

Interessiert uns die Privatsphäre unserer Mitmenschen, wenn wir einen Teil davon in den Händen halten?

Um das herauszufinden, habe ich vier USB-Speicher-Sticks präpariert und sie auf dem Campus der FH Potsdam verteilt, z.B. im Computerlabor liegen gelassen.

Der Inhalt ist konstruiert: Eine Zusammenstellung von Dingen, die in meiner Umfrage zum Überwachungsstaat (Siehe Seite 52, Frage 9) als „unangenehm, sie zu verlieren“ eingestuft wurden: Kontoauszüge, Angebote, Rechnungen, Firmendaten, Private Fotos, Adressdateien...etc. In der Grafik zu sehen sind in Orange die Antworten der



Teilnehmer zusammen mit einigen Begründungen für ihre Wahl. In Blau sind einige Ergebnisse zur Frage 8 dargestellt, bei der es um die Bewertung der Weitergabe persönlicher Daten an Dritte nach eigenem Empfinden geht. Die Zahlen sind die Ergebnisse der Daten, die man „unter keinen Umständen" an Dritte weitergegeben wissen möchte. Diese Antworten helfen mir, Daten auf den Sticks zu speichern, deren Verlust wirklich ein unsicheres Gefühl bei den Betroffenen auslöst .
Was wird also beim Finder passieren, der vielleicht erkennt, dass er sensible Dinge in den Händen hält, mit deren Hilfe er sich einen detaillierten Einblick in das Leben eines Fremden verschaffen, ihm sogar schaden könnte?
Im Fachbereich Design gibt es eine Mailingliste. Darin findet man oft den Hinweis auf gefundene Dinge. Ich hoffe, dass wenigstens zwei meiner Sticks so den Weg zu mir zurückfinden. So ergibt sich für mich die Chance, ein paar Fragen zum Umgang mit dem Fundstück zu stellen. Damit kann ich stichprobenhaft die Einstellung zum Empfinden der Privatsphäre anderer greifbar machen.
Ich denke, dass die Verlockung groß ist, rein interessehalber wenigstens auf den Inhalt des Sticks zu schauen und vielleicht sogar die eine oder andere Datei zu öffnen. Merkt ja keiner...

63 Anzahl der Teilnehmer *, die die angegebenen Daten unter keinen Umständen an Dritte weitergeben würden.

14 Anzahl der Teilnehmer *, die die angegebenen Dinge als unangenehm zu verlieren, weil sie Rückschlüsse auf die Person zulassen, angaben.

*Insgesamt beteiligten sich 79 Probanden an der Umfrage. Die Auswertung der übrigen Fragen finden Sie auf Seite 50.

Ich legte zweimal jeweils 2 Sticks aus:
Die ersten beiden waren ohne jegliche Möglichkeit, einen Rückschluss auf ihren Besitzer zu ziehen. Eine Woche nach ihrem Verlieren hatte sich niemand gemeldet. Also startete ich eine Suchanfrage an die Mailingliste, ob jemand einen Stick gefunden hat.
Auch diese blieb unbeantwortet.
Beim zweiten Anlauf hinterließ ich eine Präsentation mit meinem Namen und meiner E-Mail-Adresse auf den Sticks.
Einen dieser Sticks bekam ich zurück.

Auswertung
Fragen, die ich dem Finder gestellt habe:

1. Hast du nachgesehen, was sich auf dem Stick befindet?

2. Wenn ja: Aus welchem Grund?
Wenn nein: Wie groß war die Verlockung dazu?

3.Warum hast du den Stick nicht behalten?

4.Sind solche Daten für dich Teil der Privatsphäre einer Person?

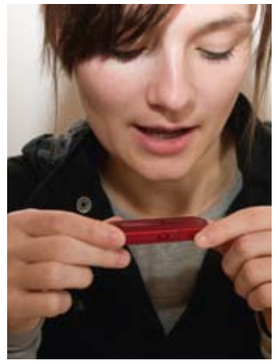
Der Finder hatte auf dem Stick nachgesehen, ob er eine Adresse oder Telefonnummer entdeckt. Er hatte von Anfang an vor, den Stick zurückzugeben, weil ihm die Daten darauf wichtig erschienen. Diese Dinge hätte er selbst nicht gern verloren. Sie gehörten für ihn selbst auf jeden Fall zu seiner Privatsphäre. Er hätte sie nicht auf einem USB-Stick gespeichert.
Über die Privatsphäre des eigentlichen Besitzers hatte er in dem Moment nicht nachgedacht.

DAGEGEN: DER MIMOSA-STICK

Eine Intervention für mehr Datensicherheit.

Aus dem Experiment „Stick-Attack“ resultierte eine kleine Idee, wie man solche Daten bei Verlust vor den Blicken neugieriger Finder schützen könnte.

Der Mimosa-Stick
Er ist mit einem Passwort zu schützen, das der Besitzer aufspricht. Der Stick ist also auf seine Stimme „geprägt“. Will der Eigentümer den Stick benutzen, sagt er das Passwort und die Schnittstelle des Sticks fährt aus. Entfernt er den Stick wieder aus dem Rechner, zieht sich sie ins Innere zurück und kann nur mit dem gesprochenen Passwort wieder aktiviert werden.
Geht der Mimosa-Stick verloren, ist er ohne Schnittstelle für einen fremden Finder unbrauchbar.
Sicher gibt es andere Wege, an die Daten zu kommen. Dies ist aber mit zusätzlichem Aufwand verbunden, den nicht jeder für einen USB-Stick betreiben will.
Somit sind die Daten des eigentlichen Besitzers etwas sicherer als auf einem normalen Stick und er hat die Chance, seinen Mimosa-Stick unangetastet zurück zu bekommen.



Wir sollten mehr Freiheit wagen…

Die CDU hat seit Jahr und Tag dafür plädiert, dass an großen Plätzen genau solche Videoüberwachung eingesetzt wird! Wenn es die CDU nicht gegeben hätte, dann würden wir heute noch ´ne lange Diskussion mit der SPD, Grünen und anderen führen – darüber, ob das nun notwendig ist oder nicht.
Das sind aber Dinge, über die darf man nicht diskutieren, die muss man einfach machen.

Bundeskanzlerin Angela Merkel auf ihrer Homepage. [31]

Bundeskanzlerin Angela Merkel auf einer öffentlichen Rede in Berlin im September 2006.[32]

DAGEGEN: PIXEL MAGIC-CAP

Eine Intervention gegen Kameraüberwachung.

Get the London Look. In der britischen Hauptstadt kommt auf 14 Einwohner eine Kamera oder anders gesagt, jeder einzelne Einwohner der Stadt wird täglich bis zu 300 mal ungewollt gefilmt,[3] Dabei sind es nicht nur staatliche Kameras, die gegen Kriminalität eingesetzt werden, sondern auch zunehmend private. Sie werden für ein subjektives Sicherheitsgefühl vor Geschäften und Wohnungen aufgestellt. Einigen Sicherheitsexperten aus Regierungskreisen kam bereits die Idee, all diese Kameras zu vernetzen und für Behörden zentral zugänglich zu machen.
Auf dieses Weise würde ein staatlich-privates Überwachungskameranetz dafür sorgen, dass Peronen nicht nur gezielt gefunden werden, sondern auch auf Schritt und Tritt verfolgt werden können.
Basierend auf diesen Fakten kam mir die Idee einer *Pixel-Tarnkappe* (Pixel Magic-Cap). Sie ist ein kleiner Beitrag für ein Stück mehr Privatsphäre, der selbstbestimmt und unauffällig eingesetzt werden kann.
Der Schirm aus einer Art Prismafolie sorgt dafür, dass sein Träger, wird er von einer Kamera gefilmt, wirkt als sei sein Gesicht verpixelt.
Seine Gesichtszüge werden unscharf und können von biometrischen Erfassungssystemen nicht mehr erkannt werden. Der Träger der Tarnkappe ist, ohne vermummt zu sein (was einen Gesetzesbruch bedeuten würde), vor den Blicken neugieriger Überwacher geschützt.
Die Tarnkappe ist so konstruiert, dass sie mit wenig Aufwand an jeder Kopfbedeckung festgemacht werden kann.
Dabei fällt sie von Weitem kaum auf und wirkt eher wie ein futuristischer Sonnenschutz.
Ihr wahrer Zweck erschließt sich wohl nur Sicherheitsbeamten.

DAGEGEN: DAS PARANOIKER-HANDY

Eine Intervention gegen Handy-Ortungsmaßnahmen.

Wer ein Handy besitzt, ist mobil und unabhängig. Er kommt in den Genuss bequemer Services und ist für andere stets erreichbar. Und er kann überall gefunden werden. Um die Erreichbarkeit des Mobiltelefons zu gewährleisten, sendet es Aktivmeldungen an das Netz. Die ermittelten Standortdaten werden an zentraler Stelle gespeichert. Im Zuge der Vorratsdatenspeicherung werden diese Daten ein halbes Jahr gespeichert bleiben.
Neue Geräte verfügen zunehmend über GPS-Ortungsmodule (Global Positioning System). Diese werden eingebaut, um z.B. bei Notrufen die genaue Position des Anrufers per Satelit zu ermitteln. Verschiedene Location Based Services setzen auf Lokalisierungsmechanismen, um Dienstleister in der Nähe des Aufenthaltsortes anbieten zu können.
Ermittlungsbehörden nutzen des weiteren „Stille SMS", um herauszufinden, wo sich ein aktiviertes Handy befindet. „Stille" SMS sind Kurzmitteilungen, welche die angeschriebenen Geräte nicht als normale Text-Nachrichten registrieren und deren Empfang sie dem Nutzer nicht wie üblich im Display melden; vielmehr quittieren sie den Empfang nur gegenüber dem Netz. So erzeugt die Polizei Verbindungsdaten beim Mobilfunkprovider, die dieser wiederum laut Gesetz „unverzüglich" zum Zwecke der Standortbestimmung auslesen und zur Verfügung stellen muss. Mit dem Hinweis auf „Gefahr im Verzug" müssen die Beamten nicht mal auf richterliche Erlaubnis warten.[33]
Meine Umfrage (Siehe Seite 50, 86) ergab, dass das Handy heute weitaus mehr ist, als ein Kommunikationsmedium. Wichtige Daten und Kontakte sind darauf gespeichert, deren Verlust viele Unannehmlichkeiten mit sich bringt. Nun soll niemand auf sein Telefon verzichten, die Vorteile eines zu haben, liegen auf der Hand. Aber ein Stück mehr Selbstbestimmung oder einfach nur die Möglichkeit, zu wissen, was das Handy gerade tut oder was mit ihm getan wird, wäre an mancher Stelle wünschenswert.
Die folgende Studie beschäftigt sich mit solchen „Eingriffsmöglichkeiten".

Das Paranoiker Handy
Grundsätzlich greifen die Interventions an den anfänglich beschriebenen Überwachungsstellen.

1. Auf dem Display gibt es eine permanente „Aktivitätsanzeige". Sie schlägt immer dann besonders aus, wenn das Handy Daten versendet oder empfängt . So können Stille SMS oder Datenversendungen an das Mobilfunknetz wahrgenommen werden.
Möchte der Besitzer diesen Prozess unterbinden, drückt er den Panic-Button, der den Datenstrom sofort stoppt, ohne dass das Handy ausgemacht werden muss.

2. Gegen das Verlieren von wichtigen Daten gibt es eine zweite, extern aufzubewahrende SD-Card, die automatisch ein Backup der internen Karte erstellt, wann immer sie in das Telefon gesteckt wird. Sie ist die doppelte Absicherung der Besitzerdaten: Vergisst der Besitzer, die zweite Karte innerhalb eines selbst gewählten Zeitintervalls in das Telefon zu stecken, geht dieses von Diebstahl oder Verlust aus und löscht automatisch die eingebaute SD-Karte.

3.Die sicherste Methode gegen unerwünschten Datenzugriff ist ein „totes Handy", also eines ohne Akku. Allerdings ist es oft umständlich, ihn zu entfernen. Das Paranoiker-Handy macht diesen Vorgang durch einfaches Schütteln möglich.
4. Für besonders skeptische Handybesitzer gibt es eine Hülle aus Edelstahldraht, die jegliche Strahlung und damit Datenaustausch unmöglich macht.

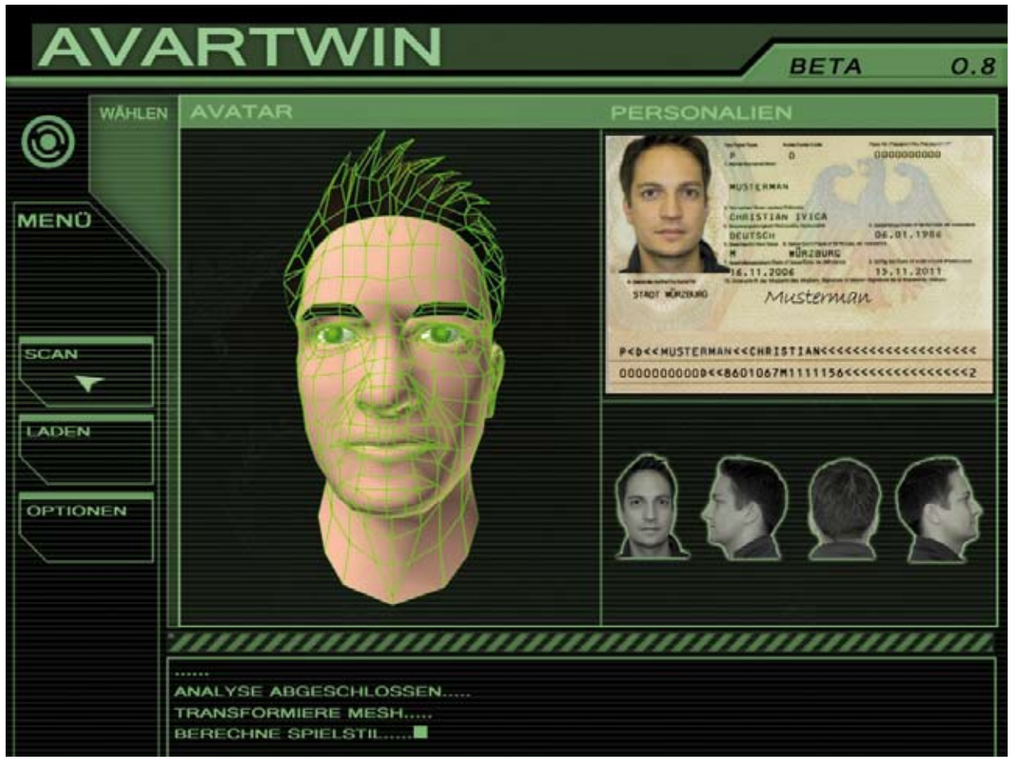
SO NICHT! SPIELEND GENERIERT

Eine Intervention für Spaß – Hand in Hand mit staatlicher Kontrolle.

Damit wir neuen Überwachungsmaßnahmen vorbehaltlos gegenüberstehen, werden sie oftmals einfach eingeführt.
Oder uns werden die Vorteile dafür so glaubhaft gemacht, dass wir uns gar nicht erst fragen, ob wir für ein bisschen mehr Überwachung auch ein bisschen mehr Sicherheit bekommen oder einfach nur ein Stück Freiheit einbüßen.
Wenn es Skeptiker gibt, findet man letztendlich ein Argument, das ihn verstummen lässt. In ganz seltenen Fällen versucht man aber auch, der Überwachungsmaßnahme ein zusätzliches bequemes Feature anzudichten, dass es eigentlich am Ende gar nicht so schlecht ist, sie zu haben.
Aus dieser Erkenntnis entstand die Idee, Maßnahmen, die eigentlich dafür gedacht waren, Daten einfacher erheben und abgleichen zu können, für einen ganz anderen Zweck einzusetzen.
Dabei fungiert das Medium, das die Daten trägt, als Ausgangspunkt: Einmal positiv für den Besitzer – als Mittel, um ein nettes Feature zu bekommen. Und zum anderen als Basis, um in weiteren Bereichen gezieltere Kontrolle zu haben.

Der biometrische Avatar.
Ein Gamer sitzt vor seinem PC und ist dabei, einen Avatar zu kreieren. Durch die Einführung der Gesundheitskarte und des biometrischen Passes gibt es die Möglichkeit, die darauf gespeicherten Daten für die Erstellung des Avatars zu verwenden. Sich mit seinem eigenen Gesicht als Held durch das Lieblingsspiel bewegen, ohne großen Aufwand – ein Traum für manchen Gamer. Und ein interessanter Service für manchen Publisher.
Der Spieler möchte einen Avatar, der sein Gesicht trägt. Er startet das Spiel. Auf dem Screen ist zu lesen: „Bitte lesen Sie Ihre Biometrischen Daten ein“. Er legt seinen Pass oder Gesundheitskarte auf ein Lesegerät. Es erscheint ein Screen: „Datenübertragung läuft“. Dann baut sich ein 3D-Gittermodell des Kopfes auf, das nach und nach mit Texturen „gefüllt“ wird. Ist der Avatar nach den Vorgaben der biometrischen Daten generiert, gibt es eine Kamerafahrt um den passbildgetreuen Kopf. Nun kann dieser auf die Lieblingsfigur montiert werden und ab gehts – mit echten Daten in die virtuelle Welt!

Scanning Data



Pass einlesen und los: (Vorab-)Screens aus dem Programm, das aus biometrischen Daten einen lebensechten Avatar generiert.

PROCEED – MIT SCHLECHTEM BEISPIEL VORAN

Die Plattform die alles weiß – ein bequemes Instrument?

Wie in der Motivation beschrieben, wollte ich in der praktischen Bearbeitung der Aufgabe nicht nur kleine Ideen umsetzen, die es dem Benutzer auf spielerische Weise ermöglichen, sich den zunehmenden sichtbaren Überwachungsmaßnahmen zu entziehen. Ich wollte etwas finden, das die Brisanz eines viel größeren Problems für alle Beteiligten spürbar werden lässt. Während der Recherche stieß ich vermehrt auf Zwischenfälle mit Daten, die ihre Besitzer ganz freiwillig veröffentlicht haben, ungeachtet etwaiger Schwierigkeiten mit Datenschutz, Weitergabe oder Missbrauch der Angaben. Sei es bei ihrem Telekommunikationsdienst oder auf Communities im Internet. Daraus ergab sich für mich der grundlegende Ansatz: Wir werden unsere Daten immer freiwillig herausgeben, wenn wir dafür einen Bonus, einen Service oder etwas mehr Bequemlichkeit erwarten können, auch wenn wir danach nicht mehr überblicken, wer unsere Profile sonst noch zu Gesicht bekommt. Um herauszufinden, ob meine Annahme sich bewahrheitet, habe ich es mir zur Hauptaufgabe gemacht, ein solches Community-Bonus-Netzwerk zu ersinnen, aufzubauen und anhand der Reaktionen meine These zu erhärten oder zu widerlegen.Das gesamte Konzept fußt auf der Eingangsidee, Interventionen für einen fiktiven Staat zu ersinnen – in diesem Fall für den Staat, dessen Überwachungsmaßnahmen unsichtbar geworden sind. Im Zuge der Beschäftigung mit neuen Überwachungsmöglichkeiten eröffnete sich mir schnell ein Weg dessen Potenzial momentan nur schwach ausgelotet scheint: Wirtschaft und Regierung finden zunehmend Mittel, sich gegenseitig Netzwerke und Technik zur Verfügung zu stellen, um Bürger bzw. Kunden für die eigenen Belange regelrecht auszuhorchen und unter Kontrolle zu halten. Und genau das wird am Ende meines Experimentes auch das Problem mit der neuen Superplattorm Proceed sein. Die „Performance Proceed“ fand bereits einige Zeit vor der eigentlichen Bachelor-Präsentation statt, damit sie nicht mit meiner Thematik in Verbindung gebracht wird. Für die Durchführung engagierte ich einen Schauspieler und briefte ihn auf die Rolle eines Marketing-Experten, der vor Studenten der FH Potsdam einen Vortrag zur neuen Studenten-Plattform Proceed halten sollte , vor allem um sie dafür zu begeistern und Beta-Tester an Land zu ziehen. Das dafür benötigte Material nebst Text stellte ich zur Verfügung. Im Vortrag selbst waren besonders die Vorteile und Bequemlichkeiten der Community hervorgehoben, damit ein positiver Eindruck entsteht, der viele dazu bringt, sich möglichst vorbehaltlos für einen Betatest anzumelden. Erst später während meiner Abschlusspräsentation werde ich Proceed als interessantes Instrument für die drohende Zusammenarbeit von Wirtschaft und Ermittlungsbehörden bloßstellen und anhand eines inszenierten „Horrorszenarios“ zeigen, wie man durch das bloße Ausfüllen und Benutzen eines Dienstes in den Fokus von Behörden geraten kann, weil übereifriges Netzwerken hinter den Kulissen, Bedienungsfehler und Fehlinterpretationen falsche Schlüsse zulassen. Hintergrund dieses Versuchs ist außerdem die Tatsache, dass für einen (meist positiven) Zweck angekündigte Technologien, Maßnahmen und Gesetze für andere Nutzungen so aufgeweicht werden, dass sie in den meisten Fällen nicht im Verdachtsmoment, sondern präventiv gegen jeden Unschuldigen ebenfalls eingesetzt werden können. Mit der unbedachten Weitergabe unserer privatesten Daten arbeiten wir aktiv an der Möglichkeit mit, jeden unserer Schritte in Zukunft nachvollziehbar zu machen, zu speichern und bei Bedarf gegen uns zu verwenden.

Wie funktioniert Proceed?

Im inszenierten Vortrag wird das fiktive Konzept aus Amerika so vorgestellt:
Als Public Private Partnership firmieren diverse internationale und deutsche Großkonzerne, um einen Fond zu unterhalten, der Studenten unterstützen soll. Das ganze geschieht unter Beteiligung der Bundesregierung.
Damit Fond und Studenten zusammenkommen, wurde Proceed ins Leben gerufen; Eine Kommunikationsplattform für Hochschulen und Universitäten, die im Frühjahr 2009 in Deutschland etabliert werden soll.
Dem angemeldeten Studenten entstehen folgende Vorteile: Für die Dauer der Nutzung erhält er eine Proceed-Card. Sie berechtigt ihn, bei Einkauf in Partnerfirmen- und filialen Rabatte von 5 – 20% zu bekommen. Gleichzeitig fungiert die Karte als Studenten- und Bibliotheksausweis, Mensa-Bezahlkarte und zukünftig auch als Fahrausweis. Auf der Plattform direkt kann er verschiedene Kommunikationskanäle bequem über ein Interface nutzen (E-Mail, SMS. Chat, Groups).
Er hat ein Instrument, um seine Vorlesungen, Teamarbeit, Termine, Materialien und Projekte zu verwalten und zu speichern.
Die Besonderheit hierbei: Interessierte Nutzer können ihre Ideen den großen Firmen über die Plattform zugänglich machen, auf Wunsch kombiniert mit den bereits existierenden Incom-Profilen*. Sie haben so die Chance, Finanzierungen für gute Konzepte zu erhalten.
Die Firmen bieten im Gegenzug Einladungen zu Events und Vorträgen, sowie für Bewerber ein Praktikumsnetzwerk und die Teilnahme an Assessmentcentern.
Motivation für dieses Engagement ist die schwindende Zahl an Studienbewerbern

Die Proceed Student´s Card.
Voller Komfort in einer Karte, dank RFID-Chip.

** Incom ist eine Entwicklung des Fachbereichs Interfacedesign an der FH Potsdam. Studenten und Professoren nutzen die Plattform derzeit als Kommunikationsmedium.*
Es gibt die Möglichkeit, für jeden belegten Kurs einen Workspace (Arbeitsraum) einzurichten, um mit Kursmitgliedern Nachrichten, Material und Informationen zu teilen.
Auf dem Schwarzen Brett ist Platz für Gesuche und Tipps aller Art.
In einem Projektarchiv kann jeder Student seine Semesterarbeiten dokumentieren und speichern. Außerdem gibt es einen Studien- und Stundenplaner, den jeder Student selbst pflegt. Es können die belegten Fächer eines Semesters sowie alle abgeschlossenen Kurse nebst der dafür vergebenen Noten und die Lehrenden eingetragen werden.

und der damit einhergehende Fachkräftemangel. Die Partnerfirmen investieren auf Proceed bereits heute in die potenziellen Mitarbeiter von morgen. Besonders an technik-affinen, zukunftsweisenden Studiengängen besteht für die Wirtschaft hohes Interesse für die Etablierung von Proceed.
Die „Gegenleistung" besteht vordergründig aus der Teilnahme an Zielgruppentests und Umfragen zu neuen Produkten, sowie Werbepaketen, die die Partner zur Awareness-Steigerung und Imageaufbesserung gezielt schalten.
Im Hintergrund spielt sich jedoch dieses Szenario ab: Nur die Studenten, die wirklich viel von sich preisgeben, können die Plattform effektiv nutzen. Je mehr Futter man Proceed gibt, desto mehr Features stehen zur Verfügung.
Es wird zwar vorgegeben, dass die erhobenen Daten die über ein normales Maß hinausgehen, nur den Firmen zugänglich gemacht werden, für die der Student dies ausdrücklich erlaubt hat. Dafür wird eigens eine „Vermittlerfirma" zwischengeschaltet. Wahrhaftig ist es jedoch so, dass alle, die im Partnernetzwerk integriert sind, Zugriff auf die Daten haben.
Und so verwundert es auch nicht, dass die Bundesregierung als Sponsor auftritt.
Die Plattform in ihrer Verbreitung ist von enormem Interesse:
Sie bündelt kompakt Profile, die über Musikgeschmack und Lieblingsfilme hinausgehen. Durch die Berechtigung, als Teil des Partnernetzwerkes auf alle eingegebenen Daten zugreifen zu können, ist ohne großen Aufwand eine leicht zu scannende Ermittlungsplattform für meinen fiktiven Überwachungsstaat geschaffen.

Material für den inszenierten Vortrag: Eröffnungsscreen, Partnernetzwerk und Visitenkarten für die Rolle des Digital Media Business Development-Mitarbeiters, der Proceed an der FH Potsdam vorstellt.

1 ***Features:*** Kommunikation (Mail/ Chat/ SMS/)
Kontakte: Enthält Profilkontakte mit Kommilitonen, Professoren, Ansprechpartnern des Sponsorennetzwerkes, Adressbuch.
Teamworkbox: Speichert aktuelle Projekte und Mitwirkende, Teamworkanfragen und ausgetauschtes Material.
Mediacenter: Speicherplatz und Back Up
Presentation Area: Hinterlegte Bewerbungen und Lebenslauf, Projektarchiv
Studienplaner: Stundenplaner, zeigt aktuelle Vorlesungen, Projekte und Professoren
Bücherzettel: Zeigt Rückgabetermine und Wartelisten, Neuerwerbungen (Erinnerung/ Benachrichtigung aufs Handy).
Kalender: Zur Organisation von Terminen (Handybenachrichtigung)
Proceed-Card: Zeigt Kartenfunktionen, Partner und Rabattsystem

2 Aktivitäts- und Vollständigkeitsanzeige des Profils

3 ***Bookmarks:*** Speichert alle Links und Suchanfragen

4 ***Offer Box:*** Zeigt Angebote aus dem Web und Partnernetzwerk, basierend auf den angegebenen Profildaten, z.B. Literaturempfehlungen zur Hausarbeit, passende Suchergebnisse zur letzten Google-Anfrage, Jobangebote u.ä.

5 ***Profile Visitors:*** Anzeige aller Besucher des Profils (nur Bild und Name).

8 ***Chatfenster:*** Zeigt alle hinzugefügten Kontakte, deren Anwesenheit und die Kommunikation über Textnachrichten.

7 ***Top 3 Contacts:*** Zeigt tagesaktuell die drei Personen an, mit denen man die meiste Kommunikation unterhält. Zu sehen sind Name, Bild, Grund der Kontaktaufnahme, Zeitpunkt des letzten Kontakts und die E-Mail-Adresse.

9 ***User Profile:*** Allgemeine Angaben, Überblick über das Studium und die Interessen des Studenten. Das Ausfüllen der meisten Felder ist freiwillig. Allerdings gilt, je vollständiger das Profil ist, desto mehr Features können genutzt werden. Die Profile sind für jeden angemeldeten Nutzer sichtbar.

10 Werbefläche für das Partnernetzwerk.

Das Interface von Proceed. Ein Premium-Profil, auf dem jedes verfügbare Feature dargestellt ist. Eine Gelegenheit für maximale Datenerfassung und Verfolgung des Inhabers, während er die Plattform nutzt.

FAZIT

Und nun?

Als ich mit dieser Arbeit begann, wusste ich nicht genau, worin sie gipfeln würde. Zwar war meine Motivation klar, nicht aber, wie ich diesem Thema gestalterisch begegen soll. Ein unendlich weites Feld tat sich vor mir auf – mit vielen Problemen und Hürden, denen man sich aktuell mehr auf politischer Seite zu stellen versucht.
Ich habe Überwachungsmethoden und ihre Beweggründe kritisch betrachtet, mich mit Technologien auseinander gesetzt und verschiedene Methoden eingesetzt, um mich dem“ Komplex Überwachung“ anzunähern. Neben der sichtbaren Überwachung mit Hilfe von Kameras und Chips begegnete mir die Möglichkeit der unsichtbaren oder sogar versteckten Überwachung, die uns heute vielleicht nicht gewahr ist, in Zukunft aber an Bedeutung gewinnen wird.
Die Idee, einen fiktiven Staat zu ersinnen und Designmöglichkeiten für oder gegen ihn zu finden, hat mich dabei stets begleitet. Als sich die Richtung abzeichnete, eine Zusammenarbeit von Staat und Wirtschaft zur vollkommenen Kontrolle über unsere Daten zu inszenieren, wurde mir die Verantwortung, die Gestalter in diesem Prozess haben, umso mehr bewusst.
Mit Hilfe eines Interfaces meine These zu belegen, zeigt, wie hoch der Einfluss eines Gestalters auf kommende Entwicklungen sein kann. Ich merkte am Feedback auf meine Eingangsidee bereits, wie wichtig einigen die Chance wäre, ab und zu selbst zu bestimmen, wann welche Dinge für wen sichtbar oder bekannt werden und, dass diese Möglichkeiten momentan schlicht fehlen. Wenn wir Benutzern verschiedenster Anwendungen uns Services nicht viel mehr Wahl- und Entscheidungsmöglichkeiten mitgeben, sorgen wir aktiv dafür, dass mit unserem Design eine unkritische „Verbrauchermentalität“ unterstützt wird, für die es lediglich wichtig ist, möglichst viele Features einfach und bequem in schicker Optik bereit zu stellen.
Dies ist für mich aber weder eine effektive noch nachhaltige Art, das Potenzial eines Interface-Designers zu nutzen. Außerdem birgt dieser Trend die Gefahr in sich, dass immer mehr Überwachungsfeatures schleichend in allen Bereichen des Lebens Einzug halten. Die guten Ideen und wegweisenden Konzepte verkommen zu Werkzeugen, die andere für ihre Zwecke verwursten.
Wir sollten also weitermachen mit verrückten Erfindungen und kreativem Output für jedes Medium. Aber gleichzeitig sollte etwas mehr Transparenz und kritische Auseinandersetzung jeden Benutzer zum Weiterdenken und mitmachen anregen.
Open Source für alles und jeden könnte das Schlagwort der Zukunft werden.
Für das spezielle Thema der Überwachung nehme ich abschließend folgendes aus dieser Bearbeitung mit:
Zum einen darf nicht der Eindruck entstehen, dass man mit Hilfe neuer Medien, Technologien und ihrer Experten eine Brücke zwischen Freiheit und der totalen Kontrolle schlagen kann. Die Sicherheit, die wir dadurch zu gewinnen versuchen, ist nicht von Dauer. Die Ursachen, die in den Augen der politischen Verantwortlichen mit immer mehr Kontrolle bekämpft werden sollen, sind nur Symptome. Die Klärung viel globalerer Konflikte wird nicht mit Hilfe von Überwachung von statten gehen.
Gute Erfindungen dürfen nicht zu einem politischen Instrument werden und es liegt auch in der Verantwortung ihrer Schöpfer, das zu verhindern.
Und wenn wir zum anderen die Entscheidung über kommende Maßnahmen gleichgültig hinnehmen und uns mit Floskeln beruhigen, werden wir zukünftig Teil einer Gesellschaft sein, in der man über uns bestimmt, anstatt uns selbstbestimmt entscheiden zu lassen.
Eine Entwicklung, die jedoch im Widerspruch zu demokratischen Grundvereinbarungen stünde. Wir müssen anfangen, nachzufragen, unbequem zu werden und den Schutz unserer Privatsphäre einzufordern, den offizielle Stellen momentan nicht gewährleisten können.
Wir haben eine Stimme, um zu sagen, wenn uns etwas nicht passt. Und wir haben die Freiheit zu Handeln – noch...

BILDNACHWEISE UND QUELLEN

Bildnachweise:

Moodboard-Bilder, Seite 16 – 17
http://matsch.binaervarianz.de/blog/uploads/rfid-tag.jpg
http://www.private-gesundheitskarte.de/funktionen/basisfunktionen/speicherung_ihrer_versichertendaten/
www.zefa.de
www.corbis.de

Filmbeispiele
Minority Report, Seite 19
Screenshots aus dem Film
Copyright: 2002, Twentieth Century Fox Film Corporation

Die Insel, Seite 21
Screenshots aus dem Film
Copyright: 2005, Dream Works

Equilibrium, Seite 23 – 25
Screenshots aus dem Film
Copyright: 2003, Dimension Films

NIN YEAR ZerO, Seite 26 – 31
Trailer Screenshots: http://www.youtube.com/watch?v=S2NS9D-Yw-4
Page Screenshots: http://www.artisresistance.com, http://viabilityindex.com, http://www.miningforlife.com, http://www.briantsunoda.com, http://hourofarrival.net, http://www.opensourceresistance.net, http://exterminal.net, http://themailstrom.com

Banksy, Seite 32 – 35
What are you looking at: http://www.flickr.com/photos/nolifebeforecoffee/124659356/
One Nation under CCTV: http://blogs.taz.de, http://i3.photobucket.com/albums/y77/iknowimasinner4/blog/banksy2.jpg
Cameras in landscape: http://www.banksy.co.uk/indoors/02.html
Deaf Society: http://www.banksy.co.uk/next/next_scroll.htm

Stasi2.0, Seite 36 – 39
Schäublone: http://www.tomsdimension.de, Mülleimer: http://systemfehler.info, Aktion IFA: http://upload.wikimedia.org JPG/800px-Stasi_2.0_auf_der_IFA_2007.JPG

Screenshot Umfrage zur Terrorabwehr, Seite 40
http://service.tagesschau.de/poll/poll_dbdata.php?oid=6637506
18.04.2007

Nacktscanner, Seite 49
http://estb.msn.com/i/4A/A258C1E2F521D85A28165E3882455A.jpg, http://upload.wikimedia.org

Google Streetview, Seite 58 – 59
http://maps.google.com/maps

Internetkameras, Seite 62 – 63
Büro: http://62.2.213.149/CgiStart?page=Multi&Language=9&Page=2&Resolution=320x240&Interval=0&Quality=Standard&Mode=Motion

Straße:
Straße: http://m-cam.uchicago.edu/view/view.shtml?imagePath=/mjpg/video.mjpg&size=1

Club: http://203.217.10.160/view/indexFrame.shtml

Logos Community-Übersicht, Seite 72 – 73
Screenshots von: http://www.studivz.net/, http://www.meinvz.net, http://www.schuelervz.net, http://www.facebook.com, http://www.myspace.com, http://www.flickr.com, http://www.youtube.com, http://www.xing.com, http://www.linkedin.com/, http://delicious.com, http://www.yasni.de, http://www.stayfriends.de, http://www.reddit.com, http://www.furl.net, http://digg.com, http://www.clipfish.de, http://de.sevenload.com, http://www.fotocommunity.de, http://vimeo.com, http://www.myvideo.de, http://view.stern.de, http://www.photocase.com, http://www.oneview.de, http://twitter.com, http://www.well.com, http://groups.google.de, http://technorati.com, http://www.yigg.de, http://nachrichten.aol.de, http://www.usenet.net/, http://www.skype.com, http://de.groups.yahoo.com/, http://de.geocities.yahoo.com, https://www.ning.com, http://mein.monster.de, http://www.lastfm.de, http://de.msn.com, http://slashdot.org, Ichat-Logo: http://www.snoobear.org

Screenshots StudiVZ, Seite 74 – 78
www.studiVZ.net

Janus-Gesicht, Seite 90 – 91
http://www.budapester.eu/Service/Links/theater_masken__Custom_.jpgwww.beadtuning.de

GamesTwin, Seite 96
Character und Spielesequenzen:
TGC – The Games Company Worldwide GmbH
Am Borsigturm 12, 13507 Berlin

Proceed Plattform, Seite 98 – 101
Anzeige Nokia: http://justanotheriphoneblog.com/
Mediamarkt-Banner: http://www.mediamarkt.de
Microsoft Office Logo: http://advertising.microsoft.com
Brands 4 Friends Bannermaterial: http://www.brands4friends.de
Logos Proceed Partnernetzwerk: www.brandsoftheworld.com
Icons: http://static.rbytes.net

Quellen

1 Stars of CCTV:
Hard-Fi
2005, Warner Music

2 http://www.heise.de/newsticker/Zehntausende-demonstrieren-fuer-Freiheit-statt-Angst--/meldung/117237
http://www.vorratsdatenspeicherung.de/content/view/142/79

3 Peter Schaar
Das Ende der Privatsphäre
Verlag: C. Bertelsmann

4 Definition Staat
http://de.wikipedia.org/wiki/Staat

5 Definition Demokratischer Staat
http://de.wikipedia.org/wiki/Demokratie

6 Trent Reznor Zitat:
(http://de.wikipedia.org/wiki/Nine_Inch_Nails)

7 Zitat über Banksy
Daily Mail, Online-Ausgabe vom 14.07.2008)

8 Banksy Biografie
http://de.wikipedia.org/wiki/Banksy

9 Definition Kommunikationsguerilla
(http://de.wikipedia.org/wiki/Kommunikationsguerilla)

The Scarlet Pimpernel
http://de.wikipedia.org/wiki/The_Scarlet_Pimpernel

11 Telekom-Spitzelaffäre: http://www.focus.de/
12 Volkszählungsboykott
http://de.wikipedia.org/wiki/Neue_soziale_Bewegungen
13 Jungle World: Volk 1.0, 6. September 2007

14 dataloo: Die Schäublone und die Meinungsfreiheit (letzter Teil), 22. Oktober 2007)
15 (http://www.diefans.de/fussball/aktuell/artikel/,Freie+Meinungs%E4u%DFerung%3F!,14058,,,,,northeast)

16 http://www.tagesschau.de/inland/meldung39010.html
http://www.tagesschau.de/inland/meldung39010.html
19.04.2007

17 http://de.wikipedia.org/wiki/%C3%9Cberwachungsstaat#Technologien.2FMethoden_zur_.C3.9Cberwachung

18 http://www.afs-rechtsanwaelte.de/urteile/artikel20-recht-auf-informelle-selbstbestimmung.php

19 http://de.wikipedia.org/wiki/Pr%C3%A4ventionsstaat

20 MacDonald, Calum (June 4, 2007). „Google's Street View site raises alarm over privacy", The Herald.

21 http://www.metrogroup.de/servlet/PB/menu/1183550_l1/index.html
http://www.welt.de/

22 Jurablog: http://www.jurablogs.com/de/und-was-schaust-du-heute-berwachungskamera-bilder

23 Definition Privatsphäre:
http://de.wikipedia.org/wiki/Privatsph%C3%A4re

24 Zitat über Gott
http://www.predigtpreis.de/predigtpreis2005/predigten2005/pyka.html

25 http://web-zweinull.de/index.php/was-ist-web-2/
http://de.wikipedia.org/wiki/Web_2.0#Web-Service

26 Tim O´Reilly
http://de.wikipedia.org/wiki/Tim_O%E2%80%99Reilly

27 http://www.spiegel.de/netzwelt/web/0,1518,537622,00.html

28 http://studivz.irgendwo.org/

29 http://www.bloggas.de/werden-einigeviele-facebook-profile-sterben/

30 Spiegel-Artikel: Terror aus dem Rechner, Ausgabe 45/2008 vom 3.11.2008.

31 http://www.bundeskanzlerin.de/nn_4922/Content/DE/StatischeSeiten/BK/Videos/2006-07-22-video-botschaft-mittelstandsinitiative.html.
32 „Auf Nummer sicher" ein halbdokumetarisches Fernsehspiel des ZDF, 2006.

33 http://www.heise.de/mobil/Ueberwachung-per-Mobilfunk--/artikel/50922

Literaturliste

Thomas Morus
Utopia
Verlag: Reclam

Aldous Huxley
Schöne Neue Welt
64. Auflage Juli 2007
Verlag Fischer

George Orwell
1984
Verlag: Ullstein

Web 2.0 - Der ultimative Guide für die neue Generation Internet
Gunther W. Kinitz
Verlag: Moses

Web 2.0. Konzepte, Anwendungen, Technologien
Tom Alby
Verlag: Hanser

DANKSAGUNG UND CREDITS

Ich bedanke mich bei allen, die mit ihrer Unterstützung zur Vollendung dieser Arbeit beigetragen haben:

Prof. Boris Müller und **Prof. Dr. Rainer Funke** für ihre Beratung und Betreuung und für den richtigen Feinschliff einiger Gedanken.

Prof. Reto Wettach für die Möglichkeit, die Proceed-Performance durchzuführen.
Dietmar Rüttiger für seinen Einsatz als Roger Fischer in der Proceed-Performance.
Jessica Pfefferkorn für die Marketing-Fachberatung für den Proceed-Vortrag.
Toni Dilsner und **Adrian Kästorf** für die Beratung und Hilfe bei der Proceed-Website.
Maik Püschel für die Organisation des Paranoiker-Handy Dummies.
Firma Dug für die Bereitstellung des Paranoiker-Handy Dummies.
Lars Lehne für die Erstellung von Versicherungsangeboten im Rahmen der Stick-Attack.
Firma AWD für die Bereitstellung von Material für die Stick Attack.
Christian Mauck für die Unterstützung bei den 3-D Sequenzen für den Biometrischen Avatar.
Firma TGC für die Bereitstellung von In-Game Material für den Biometrischen Avatar.
Sebastian Baehr für das Mitwirken im Film „Der Biometrische Avatar."
Candy Affeld für das Mitwirken im Film „Pixel Magic Cap" und der „Mimosa-Stick"-Intervention.
Anne Gunzenhäuser, **Tobias Friese** und **Thomas Kochan** für Brainstorming-Sessions und technische Beratung.
Julia Werner für moralische Unterstützung und das Mitfiebern während drei sehr anstrengender Monate.
Thomas Stieb für die tausend kleinen Gesten, die mir die Arbeit erleichtert haben.
Gabriela Skowronek für Motivation und ein offenes Ohr.
Meinen Großeltern, für die Diskussionen, die mir gezeigt haben, dass ich mit meinem Thema auf dem richtigen Weg bin. Danke an alle Teilnehmer meiner Umfragen und Experimente.

PROGNOSE

Prognose zur Umfrage „Deutschland – Überwachungsstaat?“ *

** Die hier angezeigten Ergebnisse beruhen auf Schätzungen, die vor der Auswertung der tatsächlichen Antworten von mir abgegeben wurden. Ich habe die meiner Meinung nach am häufigsten zu erwartenden Antworten angekreuzt. Die Grundlage für meine Annahme bilden Rechercheergebnisse und Erfahrungen aus Gesprächen mit Freunden zum Thema Überwachungsstaat während dieser Arbeit.*
Bitte legen Sie die Folien auf der entprechenden Seite auf die dafür vorgesehenen Markierungen, um die Ergebnisse zu sehen.