

Ein Bericht zur Überwachungsgesellschaft

Für den Datenschutzbeauftragten, vom Surveillance Studies Network

Öffentliche Diskussionsgrundlage

September 2006

Herausgeber:

David Murakami Wood und Kirstie Ball

mit Beiträgen von:

Louise Amoore
Kirstie Ball
Steve Graham
Nicola Green
David Lyon
David Murakami Wood
Clive Norris
Jason Pridmore
Charles Raab
Ann Rudinow Sætnan

London 2016: Alles unter Kontrolle¹

Auf ihrem Protestmarsch durch die Londoner Innenstadt werden der 18-jährige Ben Jones und alle anderen Kriegsgegner ständig überwacht. Kleine, ferngesteuerte UAVs (unbemannte Fluggeräte) fliegen über ihre Köpfe hinweg². Diese Spionageflugzeuge haben sich bereits während der Olympiade von 2012 bewährt. Daher setzt der Londoner Bürgermeister die „freundlichen fliegenden Augen“ (Eigenwerbung) auch weiterhin gern ein³. Inzwischen werden sie von der Bevölkerung kaum noch wahrgenommen. Kleine Kameras in Laternenmasten und Wänden auf Augenhöhe und darüber ermöglichen einen noch effizienteren Einsatz der inzwischen universal genutzten Gesichtsidentifizierung.⁴ Morphing-Software, die Bilder verschiedener Kameras kombiniert und so ein dreidimensionales Bild erstellt, befindet sich ebenfalls in der Versuchsphase, obwohl Gegner und Rechtsanwälte diese als ungenaue und unwirkliche Bilder abschreiben. Die kabellose Vernetzung ist nahezu überall möglich und erlaubt den Einsatz von Kameras ohne großartige Kästen und Verkabelung. Darüber hinaus sind sie an die intelligente Straßenbeleuchtung angeschlossen, sodass die Gesichtsidentifizierung unter idealen Lichtverhältnissen erfolgen kann. Auch automatisches Flutlicht und Extrakameras, die bei „ungewöhnlichen“ Bewegungen aktiviert werden, sind entsprechend vernetzt. Viele der wichtigen öffentlichen Gebäude, die nach 2001 mit Betonbarrieren abgeschirmt wurden, scheinen nun wieder ungehindert erreichbar. Stattdessen schützen nun sensorgesteuerte, unüberwindbare Automatikbarrieren, die nur dann aus dem Boden hochfahren, wenn sie benötigt werden, die Gebäude.

Auf dem Rückweg zur U-Bahn verirren sich Ben und sein Freund Aaron per Zufall in den Sperrbereich rund um das Regierungsviertel Westminster und werden unverzüglich von einer privaten Wachmannschaft angehalten, die dem Westminster Business Improvement District (BID)⁵ untersteht. Über ihre Handhelds⁶ und am Helm angebrachten Mikrokameras sind die Wachmänner per Fernüberwachung mit der Einsatzzentrale der Polizei verbunden. Diese Mikrokameras nehmen die beiden Jungen ins Visier⁷. Ben beugt sich dem üblichen DNA-Abstrich, der unverzüglich analysiert wird, und übergibt seinen ID-Ausweis, der durch eine Maschine gezogen wird. Die Daten erscheinen auf dem Bildschirm und einer der Beamten macht sich darüber lustig, dass ein Antikapitalist wie Ben gerade einen USA-Urlaub hinter sich hat⁸. Ben lächelt höflich. ID-Ausweise sind noch nicht gesetzlich vorgeschrieben und Aaron, der aus einer sehr christlichen Familie stammt, weigert sich, solch einen Ausweis zu beantragen. Seine Mutter sieht sie als „Zeichen des Teufels“, aber er möchte einfach nur seine Ruhe haben. Dadurch wird das Leben für ihn jedoch immer schwerer: Ohne ID-Ausweis darf er sich nicht um eine Beamtenstelle bewerben, bekommt keine Sozialhilfe oder Bafög und darf selbst in Großbritannien nicht mit dem Flugzeug oder Zug verreisen. Inzwischen fragt er sich, ob sein Protest es wirklich wert ist und wie er ohne Ausweis leben soll. Aber es kommt noch schlimmer: Als junger Schwarzer ohne ID-Ausweis steht er in den Risikoprofilen der Polizei an oberster Stelle. Daher weist die polizeiliche Einsatzzentrale die Sicherheitsbeamten an, ihn zu einer Befragung aufs Revier zu bringen⁹ ...

Von dieser Zukunftsvision des Jahres 2016 sind wir nicht mehr weit entfernt.

Im Jahr 2004 warnte der Datenschutzbeauftragte Richard Thomas, also der von der Regierung zur Überwachung der Nutzung von Personendaten eingesetzte Beamte, dass wir „uns mit schlafwandlerischer Sicherheit in Richtung Überwachungsgesellschaft bewegen“.¹⁰

Dabei leben wir dort schon längst:

- Videokameras überwachen uns überall – in Gebäuden, Einkaufszonen, Straßen und Wohngebieten. Automatische Systeme können längst Kfz-Kennzeichen (und in zunehmendem Maße auch Gesichter) erkennen.
- Elektronische Fußfesseln stellen sicher, dass sich auf Bewährung Verurteilte nicht über ihre Freigangsbedingungen hinwegsetzen und von festgenommenen Personen werden – unabhängig von der Schuldfrage – DNA-Abstriche entnommen und gespeichert. „Kriminelle Tendenzen“ werden bei immer jüngeren Menschen festgestellt.
- Ob Sozialhilfe, Gesundheitsfürsorge o.ä. – ständig müssen wir unsere Identität nachweisen. Inzwischen plant die Regierung die Einführung eines neuen Personalausweises mit biometrischen Daten (Fingerabdrücke und Iris-Scans), die auch in einer riesigen Personendatenbank gespeichert werden.
- Bei Auslandsreisen wird geprüft, überwacht und gespeichert, wer wir sind, wohin wir fahren und was wir mit uns führen. Auch an unseren Pässen geht die Neuzeit nicht vorüber: Computerchips enthalten Informationen, es liegen – ähnlich wie bei den Personalausweisen – auch schon Vorschläge für biometrische Pässe vor.
- In vielen Schulen gibt es Chipkarten, biometrische Daten überwachen den Aufenthaltsort und die Essgewohnheiten der Kinder, oder welche Bücher sie sich aus der Bücherei leihen.
- Software analysiert unser Kaufverhalten und die Daten werden an die unterschiedlichsten Firmen verkauft. Die Höhe unserer Ausgaben, unser Wohnort, unsere gesellschaftliche Stellung – all das bestimmt, wie schnell wir den gewünschten Service oder das gewünschte Angebot erhalten, wenn wir im Callcenter anrufen oder Kredite, Versicherungen oder Hypotheken beantragen.
- Telefone, E-Mails und Internet-Zugriff lassen sich überwachen und werden von britischen und amerikanischen Nachrichtendiensten auf Schlüsselwörter oder -sätze untersucht.
- Unsere Arbeit wird mehr und mehr auf Leistung und Produktivität abgeklopft, unsere Arbeitgeber interessieren sich zunehmend für unsere Einstellung bzw. unseren Lebensstil außerhalb des Arbeitsplatzes¹¹.

Die Überwachungsgesellschaft ist bereits Realität, ohne dass wir viel davon bemerkt haben.

Sie ist die Summe vieler unterschiedlicher Technologieveränderungen, vieler politischer Entscheidungen und vieler gesellschaftlicher Entwicklungen. Einige davon sind für unser tägliches Leben unerlässlich: Gesundheitswesen, Sozialeistungen, Aus- und Weiterbildung. Einige sind jedoch eher fragwürdig und lassen sich kaum rechtfertigen, da sie einschneidend und unterdrückend wirken. Dazu mag jeder seine eigene Meinung haben. Tatsächlich wissen aber die meisten Menschen kaum etwas über die Überwachungsgesellschaft. Man hält sie für Science-Fiction, nicht für das Alltagsprogramm. Deshalb findet auch kaum eine öffentliche Debatte zur Überwachung statt. Die Überwachungsindustrie ist bereits riesengroß und wächst (vor allem seit 9/11) schneller als alle anderen Sektoren¹²: Weltweit wird diese Branche auf nahezu 1 Billionen US-Dollar geschätzt. Sie umfasst ein umfangreiches Spektrum an Waren und Dienstleistungen – von militärischen Gerätschaften über Videoüberwachung (CCTV) bis hin zu Chipkarten. Die Überwachungsgesellschaft hat sich häufig langsam, geschickt und unbemerkt eingeschlichen und sich über eine willkürliche Kombination vieler kleiner Pfade einen breiten Weg gebahnt – diesen Weg müssen wir dringend besprechen und diskutieren.

Individuelle Betreuung

Geeta ist 69 Jahre alt und lebt allein in ihrer Wohnung. Zusätzlich zu den Bewegungssensoren in allen Räumen gibt es dort einen Herzschlagmonitor in ihrer Badewanne, ein Blutzuckermessgerät in ihrer Toilette und mehrere Sensoren in ihrer Küche, die einen Gasaustritt, Feuer oder Überschwemmungen melden. Ihr Notfallknopf ist direkt mit dem Callcenter der Kommunalbehörde verbunden, die bei Alarmauslösung unverzüglich anruft und nach ihr sieht. Aufgrund dieser vielen Sensoren und Kameras lebt ihre Familie allerdings in der Sicherheit, dass es ihr gut geht, und besucht sie daher inzwischen sehr viel seltener. So fühlt sie sich ein wenig einsam. Dennoch findet sie die RFID-Scanner (Radio Frequency Identification – Funkerkennung) in ihrem Kühlschrank und in ihren Schränken gut: Sobald ihr irgendwelche Lebensmittel ausgehen, bestellt der Haushaltsmanagementcomputer sie automatisch per Internet bei ihrem Supermarkt. Da die Waren ins Haus geliefert werden, geht sie nun nicht mehr selbst einkaufen. Auch an ihre regelmäßigen Gesundheits- und Gynäkologie-Checks hat sie sich gewöhnt. Was sie allerdings nicht weiß, ist, dass der britische Gesundheitsdienst NHS Geetas Ergebnisse ständig mit denen anderer gleichaltriger Frauen im ganzen Land vergleicht.¹³ Auf diese Weise lassen sich Risikofaktoren, z.B. für Herzinfarkte, genauer vorhersagen. Da Geetas Herzinfarktisiko über dem Durchschnitt liegt, bekommt sie Empfehlungen für ihre Ernährung. Doch es gibt Probleme: Der NHS muss sich ständig gegen hohe Bargeldangebote von Versicherungsgesellschaften zur Wehr setzen, die diese Gesundheitsinformationen „in bestimmten Fällen“ einsehen möchten. Da die NHS-Koffer leer sind, ist es durchaus verlockend, diese Angebote anzunehmen. Bisher fürchten sich die NHS-Bosse jedoch noch vor einem großen Skandal, wie er jüngst in Island ans Tageslicht kam. Dort war die gesamte DNA-Datenbank zu Forschungs- und Gewinnzwecken an Privatunternehmen verkauft worden.¹⁴

Und was ist so falsch an einer Überwachungsgesellschaft?

Überwachung gehört nicht zu den üblen Machenschaften fragwürdiger Bösewichter. Hinter dem Gros der Überwachung stecken gute oder zumindest neutrale Absichten: der Wunsch nach Sicherheit, Gemeinwohl, Gesundheit, Effizienz, Geschwindigkeit und Koordination. Manche Überwachungssysteme sind mit Absicht darauf angelegt, unser Verhalten oder unsere Bewegungsfreiheit einzuschränken – oft ohne unser Wissen oder Einverständnis. Und manche Überwachungssysteme zeigen diese Wirkung, ohne sie zu beabsichtigen. Dies bedeutet aber noch lange nicht, dass wir all dies hinnehmen müssen: Es ist daher von größter Bedeutung, dass wir uns der Auswirkungen dieser Überwachung sowie ihrer Folgen für unser Privatleben genau bewusst sind.

Unser Augenmerk richtet sich zunehmend auf Risiken und Gefahren und weniger auf die positive Seite gesellschaftlicher Ziele. Immer häufiger werden Alltagssituationen auf ihre „Risiken“ hin untersucht und was zuvor als außergewöhnliche Sicherheitsvorkehrung galt, ist plötzlich normal. Selten denken wir dabei an die unbeabsichtigten Konsequenzen, die nicht nur die Zugriffs- und Chancengleichheit verringern sowie Klassen-, Rassen- und Geschlechtsunterschiede oder Unterschiede in geografischer bzw. bürgerrechtlicher Hinsicht erhöhen, sondern sich einschneidend auf alle Alltagsentscheidungen auswirken.

Mithilfe von Überwachungsverfahren und -praktiken entsteht eine Welt, in der uns niemand mehr vertraut. Überwachung fördert Misstrauen.¹⁵ Arbeitgeber installieren Tastenanschlagsanzeiger in

Firmencomputern oder Routenkontrollgeräte in Dienstfahrzeugen und geben damit unumwunden zu, dass sie ihren Mitarbeitern nicht trauen. Der Sozialbeamte, der auf Sozialhilfebetrug untersucht oder nach Hinweisen für einen „Ehemann im Hause“ forscht, gibt damit zu, dass er seinen Empfängern nicht traut. Und auch Eltern, die die Aktivitäten ihrer Teenager per Webcam oder GPS-System verfolgen, erklären damit offen, dass sie ihnen nicht trauen.

Eine Überwachungsgesellschaft muss sich daher die Frage stellen, ob wir uns vom „Bedarf“ an Hightech-Lösungen für kriminelle, terroristische, betrügerische oder andere Problemhandlungen hypnotisieren lassen und völlig vergessen, diese Lösungen auf ihre Angemessenheit zu untersuchen bzw. nach anderen, nicht-technischen oder weniger einschneidenden Antworten zu suchen.

Dieses kurze Dokument sowie der beigelegte Gesamtbericht sind als Gesprächsanstoß und Inspiration für eine dringend erforderliche öffentliche Diskussion dieser Fragen gedacht. Selbst wenn wir uns für das Leben in einer Überwachungsgesellschaft entscheiden, sollte diese Entscheidung mit offenen Augen (und nicht schlafwandlerisch) gefällt werden. Die folgenden Seiten enthalten eine genauere Beschreibung der Überwachungsgesellschaft und ihrer Konsequenzen.

Was ist eine Überwachungsgesellschaft?

Unter einer Überwachungsgesellschaft versteht man eine Gesellschaft, die unter Zuhilfenahme überwachender Techniken organisiert und strukturiert ist. Überwachung bezieht sich hier auf den Zugriff auf Bewegungs- und Handlungsdaten, die im Auftrag der strukturgebenden Organisationen und Regierungen von technischen Hilfsmitteln aufgezeichnet werden. Diese Daten werden anschließend sortiert, gesichtet und kategorisiert sowie als Grundlage für Entscheidungen herangezogen, die Einfluss auf unser Leben haben. Derartige Entscheidungen beziehen sich auf unser Recht auf bzw. Zugang zu Sozialleistungen, Arbeit, Waren und Dienstleistungen sowie Strafrechtspflege, Gesundheit und Wohlfahrt und unsere Bewegungsfreiheit im öffentlichen und privaten Raum.

Auf den folgenden Seiten werden die wichtigsten Merkmale einer Überwachungsgesellschaft erläutert: Technologie, Datenfluss, Konvergenz, gesellschaftliche Kategorisierung („Social Sorting“), technologische Bindung (Lock-in) und technisches Versagen.

Technologie

Man darf an dieser Stelle nicht vergessen, dass die Überwachung im Lauf der Geschichte schon immer einen wichtigen Platz eingenommen hat und nahezu jedes autoritäre Regime (wie z.B. die DDR) hauptsächlich auf Akten und Informanten aufgebaut war bzw. ist.¹⁶ Technologische Fortschritte haben diese Überwachung jedoch verändert. Neue Überwachungsmethoden sind kleiner und leistungsstärker, sammeln, speichern und kombinieren mehr und umfangreichere Daten und stehen unverzüglich bereit. Es ist einfach unmöglich, jede Überwachungsmethode oder auch jeden Einsatzbereich in diesem Bericht zu behandeln. Statt dessen konzentriert er sich auf einige der wichtigsten Veränderungen in fünf verschiedenen Bereichen: Datenbanken, Telekommunikation, Videoüberwachung (CCTV) und Biometrik sowie Systeme zur Hausarrestüberwachung (Tagging) und Bewegungskontrolle (Tracking).

Die Datenbank

Fundament aller neuen Überwachungsmethoden ist die Computerdatenbank. Im Vergleich zu herkömmlichen Papierakten lässt sich so eine gigantische Datenflut sehr viel schneller und genauer sammeln, registrieren und querverweisen. Riesige Datenspeicher mit den Personendaten normaler Bürger sind heute wichtigstes Gut von Privatunternehmen und Behörden. Unterschiedliche

Datensätze werden miteinander verglichen und identifizieren so einzelne Personen oder auffällige Verhaltensmuster. Unter Verwendung ausgereifter Technologien ist eine explorative Datenanalyse (Data Mining) möglich, die untersuchungsbedürftige Muster an den Tag legen kann.

Jede Transaktion legt eine „Datenspur“, die zu einer Person, einem Personentyp oder einem Ort zurückverfolgt werden kann.¹⁷ Zu solchen Transaktionen zählen z.B. der Einsatz von Kreditkarten, Scheckkarten oder Handys, das Internet, Einkäufe, Internet-Suchen oder Telefongespräche. Weitere Daten können über Kundenkarten, Kundenumfragen, Fokusgruppen, Preisausschreiben, Bitten um Produktinformationen, Callcenter-Anrufe, „Cookies“ auf Webseiten, Verbraucherforen und Kredittransaktionen abgerufen werden. Diese werden häufig mit Daten aus öffentlichen Quellen überlagert, so z.B. vom statistischen Bundesamt, von gemeinnützigen Organisationen oder speziellen Unternehmen für die Datenerhebung, mit denen sich individuelle oder gemeinschaftliche „Profile“ erstellen lassen. Noch ausgereifere Methoden, bekannt als Knowledge Discovery in Databases (KDD), identifizieren versteckte Muster und prognostizieren zukünftige Transaktionen auf zunehmend persönliche Art. So bietet *Amazon* jedem Kunden z.B. Bücher oder DVDs an, die eventuell seinem Geschmack entsprechen.¹⁸

Auch im öffentlichen Dienst haben Datenbanken große Veränderungen mit sich gebracht. Das kontroverse IT-Programm *Connecting for Health* des britischen Gesundheitsdienstes NHS ist dabei das umfangreichste System Europas.¹⁹ Es wird elektronische Patientendaten mit lokalen Informationen verbinden und auf diese Weise eine landesweit komplette digitale Datenbank aller individuellen Gesundheitsdaten kreieren. Alljährlich nimmt die Polizei in England und Wales ca. zwei Millionen Menschen fest. Inzwischen müssen nahezu alle festgenommenen Personen ihre Fingerabdrücke und DNA-Abstriche abgeben. Diese bleiben – unabhängig von der Schuldfrage – in der Datenbank, sodass nunmehr fast sechs Millionen Fingerabdrücke²⁰ gespeichert sind. Die 1995 eingerichtete britische DNA-Datenbank enthält bereits die DNA von 3,45 Millionen Menschen bzw. 5,2% der britischen Gesamtbevölkerung. Dabei sei darauf hingewiesen, dass für 40% aller schwarzen Männer ein Datenbankprofil erstellt wurde, aber nur für 9% der weißen und 13% der asiatischen Männer.²¹ Weitere Datenbanken der Polizei speichern automatisch erfasste Kfz-Kennzeichen (Automatic Number Plate Recognition – ANPR), ein Register für Gewalt- und Sittlichkeitsverbrecher (Violent Offender and Sex Offender Register – ViSOR) und – nach Annahme des entsprechenden Beschlusses – auch eine landesweite Datenbank für Gesichter (Facial Images National Database – FIND). Schon bald sollen all diese Daten über den landesweiten Polizeicomputer (Police National Computer – PNC)²² miteinander verbunden werden und letztendlich nicht nur auf jeder Polizeistation, sondern (mithilfe von „Airwave“, dem neuen digitalen Kommunikationssystem der britischen Polizei) per Handheld auch jeder Polizeistreife zur Verfügung stehen.²³

Auf Basis riesiger Datenbanken, die „hinter den Kulissen“ Daten über Einzelpersonen und ihr Reiseverhalten speichern, werden Landesgrenzen zu „intelligenten Grenzen“. Profile werden zur Erstellung von Überwachungslisten für gefährliche Passagiere oder zur Identifizierung „risikoreicherer“ Gruppen herangezogen. Sogar die Erstellung rassenbezogener Profile wird offen als offizielle Politik vorgeschlagen²⁴.

Überwachung im Anflug

2016. Bei ihrer Rückkehr aus dem Urlaub in Florida steht die Familie Jones aus Großbritannien an einer völlig anderen Grenze. Die Einwanderungs- und Grenzkontrollen Großbritanniens und der USA wurden – ebenso wie die aller EU-Länder sowie der anderen G10-Industrieländer – an ein und dasselbe internationale Privatkonsortium (BorderGuard)²⁵ vergeben. Die Angst vor illegalen Einwanderern sowie die Regierungsrhetorik, die von einem „Krieg gegen den Terror“ spricht, veranlasste diese Regierungen zur Einführung „intelligenter Grenzen“. Die Passkontrolle besteht nun aus

einer Reihe von Kameras und Scannern, die Bilder von Gesicht, Iris und Fingern machen und diese mit den Daten des biometrischen Standardpasses (bzw. im Falle Großbritanniens des ID-Ausweises) vergleichen, den alle G10-Länder und die EU²⁶ längst eingeführt haben. Der eingebaute RFID-Chip enthält nun alle Angaben zu Staatsangehörigkeit und Einwanderung, Visa-Informationen und strafrechtliche Daten sowie Gesundheitsdaten. Diese werden zeitgleich mit den landesweiten und internationalen Datenbanken verglichen. Auch eine Fülle an datengeschürften Informationen zum Kaufverhalten, die BorderGuard von darauf spezialisierten Unternehmen²⁷ erhält, werden damit abgeglichen. Für die meisten Familienmitglieder geht dieser Prozess schnell vonstatten. Für Großmutter Geeta ist er allerdings nicht ganz so problemlos: Pakistan hat das vollständige Programm der „intelligenten Grenzen“ noch nicht ratifiziert, und Geeta besitzt noch keinen biometrischen Pass. Daher muss sie stundenlang Schlange stehen und mehrere Extradurchsuchungen und Befragungen über sich ergehen lassen. Trotz ihres britischen ID-Ausweises löst auch das „asiatische“ Aussehen von Mutter Yasmin einen Alarm aus, sie muss sich bei einer Befragung rechtfertigen. Am Zoll werden alle Reisenden elektronisch abgetastet, also einer virtuellen Leibesvisitation unterzogen ...²⁸

Telekommunikation

„Telekommunikation“ bezieht sich nicht nur auf das herkömmliche Festnetz für Telefongespräche und Faxe, sondern auch auf Handys (inklusive Sprachübertragung, SMS, Bilder, Töne und Standortinformationen) sowie Computerkommunikation (z.B. Internet, d.h. Breitbandtechnologie usw.). Zu einer Zeit, als es ausschließlich staatliche Analogtelefone gab, wurden die Apparate zur Überwachung „angezapft“ (gewöhnlich von der Polizei oder dem Nachrichtendienst). Seitdem haben sich drei Dinge geändert: die Telefontechnologie selbst (Handys, Faseroptik, kabellose Verbindung usw.), die Kombination von Telekom- und Computerspeicherung und -bearbeitung (E-Mail, Webseiten usw.) sowie die Gründung privater Telekom-Unternehmen. Diese Veränderungen führen zunehmend zu einer Konvergenz der Technologien und zu einer Art Wechselwirkung, bei der die unterschiedlichsten Technologien zusammenarbeiten.

Damit all diese Technologien auch funktionieren, muss ein Signal- oder Datenaustausch zwischen einzelnen Geräten stattfinden. Und genau dieser Austausch kann überwacht werden. So lässt sich der Standort eines Handys feststellen, so kann der Besuch einer Webseite vom Internet-Anbieter katalogisiert werden. Je umfangreicher die Verbindung zwischen den unterschiedlichen Telekommunikationsmethoden ist, desto mehr Informationen werden verfügbar. Das Gesetz verlangt inzwischen die Aufbewahrung dieser Daten zu Analyse Zwecken: Im Februar 2006 beantragten sowohl die EU als auch das britische Innenministerium, diese Daten bis zu zwei Jahre zu speichern und zur polizeilichen Fahndung zu nutzen.

Darüber hinaus filtern die Länder einen Großteil des Telefon-, Telex-, E-Mail- und Faxverkehrs aus „nationalem Interesse“ (d.h. aus Gründen der Sicherheit und Wirtschaft). Das „ECHELON-System“, das weltweit einsetzbare Überwachungsnetz des amerikanischen Nachrichtendienstes NSA, unterhält in Menwith Hill in Nord-Yorkshire (GB) eine riesige Basis, die routinemäßig die gesamte Telekommunikation in Großbritannien auf Schlüsselwörter und -sätze untersucht und zunehmend ausgereifere Algorithmen für hochwertige Sprach- und selbst Bedeutungserkennung einsetzt²⁹.

Virtuelle Überwachung

Nachdem Ben von der Polizei freigelassen wird, macht er sich auf den Heimweg. Sein Handheld³⁰ wird nun jedoch über Galileo verfolgt³¹. Außerdem wird sein Name zur Überwachung seiner Kommunikation auf eine Liste gesetzt, sein Internet-Anbieter erhält

eine automatische Anordnung gemäß „RIP 2 Gesetz 2009“, nach dem seine gesamte Internet- und E-Mail-Kommunikation gespeichert und an die Polizei weitergeleitet werden muss³². Da das Gros der Telefonie inzwischen bereits über das Internet läuft (und herkömmliche Festnetzleitungen von der Bildfläche verschwinden), trifft dies auf Bens gesamte Kommunikation zu. Ein unvorhergesehenes Ergebnis der Überwachung von Bens Kommunikation ist die Tatsache, dass Bens jüngerer Bruder Toby, der sich von Zeit zu Zeit der Anschlüsse seines Bruders bedient (vor allem, weil ihm Cracking³³ Spaß macht), ebenfalls in die Überwachung einbezogen wird. Für Toby spielt sich das Online-Leben hauptsächlich in Massively Multiplayer Online Games (MMOGs) ab. Das sind virtuelle Welten mit eigenen Regeln und völlig anderen, alternativen Wirtschaftsgefügen³⁴. Doch die Überwachungsgesellschaft gibt es hier auch schon. Diese Daten- und Verhaltenswelten der „Online-Avatare“ werden vor allem von Unternehmen überwacht, die nach neuen Geschäftschancen in aufsteigenden Realmärkten suchen. Es gibt eine völlig neue Kategorie von firmeneigenen Spielern, deren Ziel einzig und allein die Untersuchung der Gepflogenheiten bestimmter Personen über ihre „Avatare“ sowie die anschließende Vermarktung von virtuellen und realen Produkte innerhalb und außerhalb dieser Welten an diese Spieler ist³⁵. Auch die Polizei experimentiert schon mit Software, die diese virtuellen Welten überwacht und „Avatare“ identifizieren kann, deren ungewöhnliches Verhalten auch auf reale kriminelle Tendenzen der Spieler schließen lässt³⁶. Natürlich sind die Spieler selbst gegen diese Verfahren, da sie – laut Eigenaussage – ihre Flucht in die virtuellen Welten sehr wohl von der Realität unterscheiden können.

Videoüberwachung

Ihre Anfänge fand die Videoüberwachung (CCTV) zwar schon in den 60er Jahren des 20. Jahrhunderts, doch das wahre Wachstum fand Ende der 80er Jahre statt – ausgelöst von dem Versuch, die Verödung innerstädtischer Einkaufsbereiche aufzuhalten, sowie von der Angst vor Terrorismus, Kriminalität und Rowdytum. Inzwischen gibt es wohl rund 4,2 Millionen CCTV-Kameras in Großbritannien, d.h. eine Kamera je 14 Einwohner³⁷, eine einzige Person kann täglich von mehr als 300 Kameras aufgenommen werden.³⁸ Diese CCTV-Infrastruktur kostete den Steuerzahler im vergangenen Jahrzehnt laut Schätzungen rund 500 Millionen GBP³⁹. Dennoch kam eine Studie des britischen Innenministeriums zu dem Schluss, dass „die bewerteten CCTV-Programme insgesamt nur geringen Einfluss auf die Kriminalitätsraten hatten“.⁴⁰

Die Digitalisierung erlaubt den zunehmend automatischen Einsatz von CCTV-Anlagen. Kfz-Kennzeichen dienen zur Identifizierung des Fahrzeughalters. Die Kameraüberwachung von Geschwindigkeitsbegrenzungen steigerte sich von gerade einmal 300.000 Strafzetteln im Jahr 1996 auf mehr als zwei Millionen im Jahr 2004 und bringt dem britischen Staat damit Bußgelder in Höhe von 113 Millionen GBP ein.⁴¹ Dieser Anstieg staatlicher Überwachung sorgt für einen Strom negativer Presse⁴² – und das, obwohl die Geschwindigkeitsüberwachung per Kamera (ganz im Gegenteil zur CCTV-Überwachung) die Zahl der Todesfälle und Verletzten im Straßenverkehr deutlich reduziert.⁴³

Diese Überwachung der Verkehrsteilnehmer ist auf eine umfangreiche und schnelle Intensivierung angelegt. Im März 2005 forderte der britische Verband leitender Polizeibeamter (Association of Chief Police Officers) eine landesweite Vernetzung von Kfz-Kennzeichenlesern, „unter Einsatz der Polizei, örtlicher Behörden, des britischen Straßenverkehrsamtes (Highways Agency) sowie der Kameras sonstiger und wirtschaftlicher Partner“⁴⁴, inklusive der Integration bereits installierter Kameras in Stadtzentren und Einkaufszonen⁴⁵, mit einem nationalen Datenzentrum für automatisch erfasste Kfz-Kennzeichen. Dieses Zentrum würde über eine Verarbeitungskapazität von 35 Millionen automatisch erkannter Kfz-Kennzeichen pro Tag verfügen und ließe sich bis 2008 auf 50 Millionen steigern. Alle Daten würden zwei Jahre lang gespeichert.

Elektronisch beschleunigt

Wenn Gareth von seinem Anwesen fährt, öffnen sich die schmiedeeisernen Tore automatisch. Eine Kamera registriert die genaue Abfahrtszeit sowie die Anzahl und Identität der Fahrzeuginsassen. Im Straßenverkehr funktioniert die automatische Kfz-Kennzeichenerkennung ANPR bereits seit 2008, und inzwischen gibt es so viele Kameras, dass es sich wirklich nicht mehr lohnt, sie mit Scannern oder speziellen Landkarten aufzuspüren. Der Handheld, den Gareth an sein Fahrzeug anschließt, ist sowieso direkt mit dem weltweiten Satellitennavigationssystem Galileo sowie mit staatlichen Staukameras verbunden, die ihm die schnellste Route berechnen. Die Berechnung der kürzesten Route zahlt sich außerdem auch finanziell aus, da das ANPR-System die Kilometerzahl berechnet und automatisch die fällige Straßengebühr von Gareths Bankkonto abbucht.⁴⁶

Biometrische Daten

Nahezu alle neuen ID-Systeme nutzen die eine oder andere Form biometrischer Daten oder Körpermerkmale: Fingerabdrücke, Iris-Scans, Gesichtskonturen und Hand-Scans werden in verschiedenen Pässen bzw. Personal- oder ID-Ausweisen längst eingesetzt. Häufig werden diese biometrischen Daten als unfehlbar dargestellt. Man geht davon aus, dass ihre Genauigkeit optimiert und betrügerische Aktivitäten damit reduziert werden können. PIN-Nummern und Passwörter kann man vergessen oder verlieren. Körpermerkmale stellen jedoch eine konstante, direkte Verbindung zwischen Aufzeichnungssystem und Person her. Seit 9/11 werden sie vor allem in den USA gefördert – daher forciert Amerika auch die Ausarbeitung gemeinsamer Normen für biometrische Pässe.

Überall in öffentlichen Behörden und Privatunternehmen finden sich biometrische Zugangskontrollen (vor allem über die Stimme oder mit Hand-Scans). Auch auf einigen Flughäfen werden sie bereits eingesetzt, so z.B. der Iris-Scan „Privium“ auf dem niederländischen Flughafen Schiphol. Doch die Biometrik kommt in zunehmendem Maße auch auf die Straße: Britische Städte experimentieren mit automatischer „Gesichtserkennungssoftware“ – so in Newham (London), Birmingham, Tameside, Manchester und anderswo. Im Freien und auf überfüllten Straßen mit vielen sich schnell bewegend Menschen funktionieren die Gesichtserkennung und auch andere biometrische CCTV-Anlagen noch nicht perfekt. In ihre Weiterentwicklung werden jedoch Riesensummen investiert.

Ihre Gesundheit ist unsere Sache!

Im Jahre 2016 arbeitet Gareth als Manager eines Callcenters. Seit 2006 hat sich nicht viel geändert: Die Mitarbeiter werden kontinuierlich von einem Computer überwacht, der jede ihrer Handlungen und die Länge ihrer Arbeitsschritte aufzeichnet. Bei der Personalbeschaffung und Berechnung von Sozialleistungen wurde die Überwachung jedoch intensiviert. Die Mitarbeiter müssen sich nun einer Reihe von biometrischen und psychometrischen Tests unterziehen und Fragen zu ihrem Lebensstil beantworten. Gareth legt Wert darauf, dass das Lifestyle-Profil eines Mitarbeiters dem der Kunden entspricht, um einen besseren Kundendienst bieten zu können.⁴⁷ Außerdem achtet er darauf, dass seine Mitarbeiter keine gefährlichen Sportarten (wie Rugby oder Mountainbiking) ausüben, da sie sich dabei leicht verletzen und lange krankgeschrieben werden könnten. Biometrische Tests, also Mundabstriche und Urinproben, werden mithilfe eines preiswerten Sets unverzüglich von der Firmenkrankenschwester analysiert. Der Arbeitgeber kann also sofort feststellen, ob der zukünftige Angestellte Gesundheitsprobleme hat oder Drogen nimmt und so die Produktivität des Unternehmens gefährden würde. Gleichzeitig kann das Unternehmen je nach Gesundheitszustand eines Mitarbeiters ein flexibles Paket an Sozialleistungen zusammenstellen. Manch übereifriger Kandidat liefert bereits freiwillig Gesundheitsinformationen, sodass das Unternehmen dazu übergegangen ist, Lebensläufe ohne diese Daten gleich zu ignorieren. Die Sorge um den Gesundheitszustand ihrer Mitarbeiter lässt viele Unternehmen proaktiv handeln – bei Vorlage ihrer RFID-Chipkarte, die sie auch am Arbeitsplatz benutzen, erhalten die Mitarbeiter vergünstigten Eintritt zu den Sportstudios vor Ort. Die Nutzung der Sportstudios wiederum wird in der elektronischen Personalakte gespeichert. Mitarbeiter, die sich dort nicht regelmäßig fit halten, werden z.T. bei ihren Jahresgesprächen auf ihren Lebenswandel angesprochen. Regelmäßige psychometrische Tests zeigen der Geschäftsleitung außerdem, ob die Einstellung des Mitarbeiters der Unternehmenskultur und den Unternehmenswerten entspricht.

Ortung (Locating), Bewegungskontrolle (Tracking) und Hausarrestüberwachung (Tagging)

Die Überwachung befasst sich zunehmend mit der Bewegungskontrolle von Personen: über GIS (Geographic Information Systems), GPS (Global Positioning Systems), RFID-Chips, intelligente ID-Ausweise/Personalausweise, Transponder oder die Funksignale von Handys bzw. tragbaren Computern.

Sowohl GPS als auch RFID (Funkerkennung) werden immer häufiger als Lösung im Bereich der Strafverfolgung bzw. im Personalwesen angesehen. Bei Haftstrafen auf Bewährung wurde die elektronische Überwachung ebenfalls eingeführt, und im Zeitraum 2004/5 erhielten 631 Erwachsene und 5751 Jugendliche (manche nicht älter als zwölf Jahre) eine elektronische Fußfessel, mit der sie ihren Prozess zu Hause und nicht in Untersuchungshaft abwarten konnten.⁴⁸ Auch Gefangene, die ihre Haftstrafe abgesessen haben, werden verstärkt elektronisch überwacht, sei es als Bedingung ihrer vorzeitigen Entlassung im Rahmen einer Hausarrestüberwachung per Fußfessel (Home Detention Curfew Scheme)⁴⁹ oder einer bedingten Haftentlassung.⁵⁰

Noch vor Kurzem beschränkte sich der Einsatz von RFID auf große Schiffscontainer, Konsumgüter und diverse Chipkarten. Die breite Öffentlichkeit hat den sich hier vollziehenden Wandel, nämlich die Implantation in Lebewesen, kaum wahrgenommen. Im Rahmen des PETS-Programms ersetzen Chips mit Schutzimpfungsinformationen bzw. Besitzerdaten seit dem 28. Februar 2000 die EU-Quarantäneanforderungen für Haustiere. Inzwischen wurde dieses Programm auch auf außereuropäische Länder ausgeweitet⁵¹. Der erste Einsatz von RFID-Chips beim Menschen fand in

den USA statt: Sie wurden älteren Mitbürgern mit degenerativen Hirnkrankheiten eingepflanzt. Inzwischen tragen ca. 70 Personen ein Implantat mit sich herum und erleichtern den Pflegern damit ihre Ortung⁵². Forscher und Technikfreaks setzen sich seit Jahren selbst Chips ein⁵³ und mindestens eine spanische Nachtclub-Kette bietet ihren Besuchern bereits bestimmte Privilegien durch Implantate⁵⁴. Im Februar 2006 machten diese Entwicklungen einen Riesenschritt nach vorn, als ein Wachunternehmen in Ohio (USA) zwei seiner Mitarbeiter RFID-Chips einsetzte, um ihnen Zutritt zum Unternehmensgelände zu gewähren⁵⁵. Auf einigen Technologie-Webseiten wird bereits ernsthaft gefordert, allen Menschen einen derartigen Chip einzupflanzen.

Für Unternehmen liegt die zukünftige Nutzung von RFID-Chips und GPS-Systemen hauptsächlich in der Erstellung kundenspezifischer Marketingmaterialien in Echtzeit, so z.B. Rabatte auf tragbare Elektronikgeräte für Einzelhändler an einem bestimmten Standort. Die kontinuierliche Weiterentwicklung des Einsatzes von Echtzeit-Standortdaten in Verbraucherprofilen bildet eine weitere Datenschicht, die Unternehmen bei der gezielten Ausrichtung ihrer Marketingkampagnen auf individuelle Verbraucher unterstützt. Gleichzeitig wird hiermit die Bewegungskontrolle im Rahmen der Strafverfolgung sowie anderer staatlicher Überwachungsmaßnahmen möglich.

Die neue Markenlandschaft – Brandscape

Wenn Familie Jones im Jahre 2016 ihr Einkaufszentrum besucht, stößt sie dort nach wie vor auf Videoüberwachung (CCTV) und Wachleute. Und doch hat sich einiges geändert: Neben der Kriminalitätskontrolle haben sich die dreidimensionale Modellierung der „Brandscape“⁵⁶ sowie wechselnde Werbung je nach den unterschiedlichen Verbraucherströmen zu strategischen Prioritäten entwickelt. Die Einzelhandelsketten geben dem Einkaufszentrum Einblick in die riesige, gemeinsame Datenbank, die (über Kundenkarten gesammelte) Käuferinformationen enthält. Das System basiert auf RFID-Etiketten an der Kleidung, allgegenwärtigen Scannern und Verbraucherdaten. Die Scanner in den Ladentüren protokollieren die individuellen Identifikationsdaten der RFID-Chips, die sich in der Kleidung der Verbraucher befinden. Intelligente Reklamewände in Augenhöhe werben für ausgewählte Produktserien, die in Echtzeit an jeden Verbraucher angepasst werden. Sara freut sich über das neueste Download ihrer Lieblingsband auf dem Bildschirm, während Toby Informationen über spezielle Modifikationen seiner geliebten Online-Welt sieht. In der Nähe bestimmter Geschäfte wird dem Verbraucher individuelle Werbung auf seinen Handheld gesandt.

Umsatzstarken Kunden wird das neue bargeldlose System angeboten, das „wertvollen“ Kunden⁵⁷ stattdessen ein Chip-Implantat vermittelt.⁵⁸ Zwar kostet es 200 GBP, doch bei all den Rabatten in den Geschäften⁵⁹ amortisiert sich das schnell. Man kann einen Betrag auf den Chip laden und dann in den unterschiedlichsten Läden einfach seinen Arm scannen lassen. Kredit-, Bank- oder Kundenkarte gehören der Vergangenheit an. Chip-Kunden haben Zutritt zu VIP-Lounge, Wellness- oder Massageeinrichtungen vor Ort. Laut Werbung sind die Verbraucher mit diesem „bargeldlosen“ System sicherer vor Straßenräubern und Taschendieben oder auch Kreditkartenbetrug. Angeblich hat zwar ein Straßenräuber im Parkhaus einem Verbraucher seinen Chip aus dem Arm geschnitten, doch das ist laut Betreiber nur ein Gerücht. Der Vater von Gareth hatte sich zwar schon für einen solchen Chip entschieden, sah dann jedoch im Fernsehen, dass sie von Computerviren angefallen werden können. Seine Sorge gilt vor allem den Konsequenzen eines Betrugsverdachts – heutzutage wird das sehr, sehr ernst genommen.

Ausgereifere Prognose-Algorithmen auf Basis individueller Verbraucherprofile führen nämlich dazu, dass schon ein Anruf von der Bank genügt, um ihn schuldig zu sprechen: Alle Karten werden automatisch deaktiviert und der Verbraucher muss der Bank unabhängige Beweise seiner Identität und seines Wohnorts vorlegen.

Datenflüsse

Die von den Überwachungssystemen gesammelten Daten fließen durch die Computernetze. Viele Menschen geben ihr Einverständnis für die Erfassung ihrer Daten an einer Stelle, doch was passiert mit diesen Daten, wenn sie auf einen anderen Computer übertragen werden?

Weder die Öffentlichkeit noch die mit der Weiterleitung unserer Daten betrauten Stellen wissen genau, wohin diese Daten wandern.

Schleichende Funktionsausweitung

Überwachung folgt einer eigenen Logik. Diese Logik muss jedoch in Frage gestellt, untersucht und geprüft werden – vor allem dann, wenn Daten von einer Station zur nächsten fließen und Informationen, die zu einem bestimmten Zweck gesammelt wurden, an einem neuen Standort neuen Zwecken dienen. Ein Beispiel: Die individuellen Transportdaten auf der Londoner Oyster-Card (für den öffentlichen Nahverkehr) werden bereits verstärkt von der Polizeifahndung angefordert.⁶⁰ Inzwischen wenden Sicherheits- und Nachrichtendienste bei der Terroristenfahndung nicht nur die Datenschürfmethode der Verbraucherprofilanalyse an, sie bedienen sich auch genau der Daten, die zur Erstellung dieser Profile herangezogen werden.

Auch die medizinische Diagnostik schleicht sich schrittweise in immer breiter angelegte Kontexte ein und schwächt damit gleichzeitig die Prognosevoraussetzungen für eine positive Diagnose: Falsche Diagnosen können leicht zu Nachteilen für die diagnostizierte Person führen. Am Arbeitsplatz geben die Überwachungssysteme vielleicht mehr Informationen her als geplant und die Geschäftsleitung könnte in Versuchung kommen, diese Überwachung auch ohne Einverständnis der Mitarbeiter auszudehnen und damit größeren Einfluss auf Lohn- oder Beförderungsentscheidungen zu nehmen.

Konvergenz

Eine immer größere Zahl von Systemen wird mit Blick auf diese Datenflüsse entwickelt. Eingebaute Wechselwirkungsmechanismen führt zu einer steigenden Konvergenz zwischen den Überwachungstechnologien. Völlig unvorhergesehen und unkontrolliert können neue Produkte entstehen. So steigt der Druck, ID-Ausweise/Personalausweise zu entwerfen, die mehreren Zwecken dienen: Grenzüberschreitung, Betrugskontrolle, Zugriff auf staatliche Informationen und ggf. sogar kommerzielle Zwecke (Videoverleih) oder halbkommerzielle Zwecke (Büchereien). Die Manager dieser Identitätsdatenbanken erhalten damit eine unsagbar große Macht über Akten, deren Informationen Leben verändern können.

In Richtung einer allgegenwärtigen Überwachung

Technologie wird vor allem dann besonders wichtig, wenn sie immer und überall vorhanden ist und ihre – nahezu unsichtbare – Existenz als gegeben vorausgesetzt wird. Im Alltag durchqueren wir immer mehr „Übergänge“, die eine enge Zusammenarbeit *sowohl* elektronischer als auch physischer Bestandteile voraussetzen: die Kombination von CCTV, biometrischen Daten, Datenbanken und Bewegungskontrollen. Wir werden mehr und mehr jederzeit und überall überwacht: Unsere Überwachung ist allgegenwärtig.

Gesellschaftliche Kategorisierung

In einer Überwachungsgesellschaft ist die gesellschaftliche Kategorisierung („Social Sorting“) ganz normal. Die Analyse und Kategorisierung staatlicher und kommerziell genutzter Riesendatenbanken mit Personenangaben führt zur Aufteilung in Zielmärkte und Risikogruppen⁶¹. Und wer einmal klassifiziert wurde, kommt aus dieser Schublade nicht so schnell wieder heraus. Seit 9/11 hat diese Kategorisierung vielleicht zu einem sichereren Luftraum geführt (was sich jedoch nicht beweisen lässt), gleichzeitig hat sie aber auch grobe Profilgruppen (z.B. Muslime) entstehen lassen und Nachteile, Härten und sogar Folter mit sich gebracht.

Die gesellschaftliche Kategorisierung definiert die Überwachungsgesellschaft immer mehr. Sie ermöglicht den unterschiedlichen Gesellschaftsgruppen unterschiedliche Chancen und führt auf oft raffinierte und zuweilen unbeabsichtigte Weise zu einer Neuordnung der Gesellschaft, zu Politik ohne demokratische Debatten. Unsichtbare, als selbstverständlich hingenommene Systeme zur Begleichung der Straßengebühr oder für intelligente öffentliche Verkehrsmittel sind sicherlich nützlich, sortieren eine Stadt jedoch in zwei Gruppen: Jene, die sich relativ frei bewegen können und jene, die damit Schwierigkeiten haben. Gleichzeitig lassen sie sich zur Kriminalitätskontrolle und für die nationale Sicherheit einsetzen. Niemand hat diese Systeme direkt gewählt. Sie werden

aus Gründen größerer Effizienz und Effektivität im öffentlichen Dienst eingesetzt, oder auch auf Druck der Technologieunternehmen, dem von der Gesellschaft zunehmend wahrgenommenen „Risiko“ und dem Gedanken, dass wir nichts unversucht lassen sollten, um großen Gefahren vorzubeugen.

Kinderkontrolle

Im Jahre 2016 sind Überwachung und Bewegungskontrolle längst ein entscheidender Bestandteil der Erziehung.⁶² Im Anschluss an einige landesweit dokumentierte Fälle, in denen Schüler sich verlaufen haben bzw. verletzt oder getötet wurden, liegt vielen Schulen (vor allem Grundschulen und sogar Kindergärten) nun daran, den Aufenthaltsort ihrer Schüler zu kontrollieren und so strafrechtliche Verfolgungen zu vermeiden.⁶³ Als Antwort auf die Regierungspolitik einer frühen Identifizierung von Problemkindern, dem Kampf gegen Schulschwänzer und einer Initiative zur Verbesserung der Lernkonzentration begannen Grundschulen mit Drogentests – wohl auch, um in den allgegenwärtigen Schulranglisten aufzusteigen.⁶⁴ In der Schule von Toby Jones wurde ein bargeldloses Kartensystem eingeführt, mit dem die meisten Familien die Essgewohnheiten ihrer Kinder überprüfen. Nach drei Jahren kaufte der Supermarkt NSC das Kartenunternehmen als Einstieg in den lukrativen Jugendmarkt und steigerte seine Markenbekanntheit durch den Kauf von Lernmitteln. Die Eltern wurden gebeten, die Karte ihrer Kinder durch die Supermarktkassen zu ziehen. So ließen sich Schule, Schüler und Eltern identifizieren und NSC lieferte dann weitere Lernmittel an diese Schule – jeweils in Anlehnung an die Höhe der elterlichen Einkäufe. Einige der NSC-Hauptlieferanten⁶⁵ installierten Verkaufsautomaten in den Schulen. Tobys Schule nimmt auch heute noch an dem NSC-Programm teil und auf allen neuen Lernmitteln prangt stolz der Markenname „NSC“. Die Kommunalbehörde untersucht die an Tobys Schule verzehrten Lebensmittel und nutzt diese Informationen dann für verschiedene Kampagnen zu „gesunder Ernährung“. Die Karte wurde mehr und mehr in den Alltag integriert. Heute enthält sie Daten zu den von den Kindern gekauften Mahlzeiten, aber auch Informationen zur Anwesenheit der Kinder, ihren Leistungen, außerschulischen Aktivitäten, Ergebnissen von Drogentests und Internet-Zugriff. Darüber hinaus werden sie im Fach Sozialkunde eingesetzt. Die gestiegene Überwachung hat den Schulen und Schülern sicherlich deutlich messbare Vorteile gebracht, doch gleichzeitig akzeptieren diese Kinder heute immer intensivere und aufdringlichere Überwachungsmethoden, Bewegungskontrollen und die Überprüfung ihrer Ess- und Aufenthaltsgewohnheiten als ganz normal ...

Technologische Bindung (Lock-in)

In punkto Überwachung wird es sicherlich auch einige technologische Gegenentwicklungen geben: Moderne Datenschutztechnologien (Privacy-enhancing Technologies – PETs) könnten die Überwachung einschränken oder drosseln und sollten deshalb, wo immer dies angemessen erscheint, eingesetzt werden. Dennoch sollten weder technisches Versagen noch PETs dafür sorgen, dass schlicht und einfach „bessere Technologien“ entwickelt werden. Je mehr sich Staat, Institutionen, Einzelpersonen und die Gesellschaft als Ganzes auf Überwachungstechnologien verlassen, desto mehr entsteht eine technologische Bindung, andere Möglichkeiten mit dem gleichen Ziel werden kaum noch in Betracht gezogen. Es entsteht ein Verständnisgefälle, das unsere Abhängigkeit von Experten außerhalb des demokratischen Systems verstärkt. Sind die ID-Ausweise/Personalausweise z.B. erst einmal eingeführt, intensiviert sich automatisch die staatliche Abhängigkeit von den Organen, die das technologische und wirtschaftliche Know-how dafür stellen.

Wir sollten Angebote, die sogenannte technische Probleme ausschließlich mit technischen Lösungen angehen, mit Vorsicht genießen. Wie sich zeigen wird, ist die reale Überwachungsgesellschaft viel zu komplex für solch oberflächliche Reaktionen. Wir müssen uns also fragen, ob dem Staat die notwendigen Werkzeuge für eine sinnvolle Steuerung zunehmend komplexer Überwachungstechnologien und -methoden überhaupt zur Verfügung stehen. Können wir die Geister, die wir riefen, wieder loswerden?

Technisches Versagen

Natürlich verspricht uns die Technik meist mehr als sie tatsächlich halten kann. Die biometrischen Anlagen für das amerikanische USVISIT-Programm wurden z.B. aus logistischen Gründen von den geplanten Iris-Scans auf digitale Fingerabdrücke reduziert.⁶⁶ Und auch die biometrischen Elemente des britischen e-Borders-Programms machten schon bei der Implementierung Probleme⁶⁷. In der Realität liegt die Gesichtserkennung noch weit unter dem gewünschten Leistungsniveau. Das britische Amt für polizeiliche Führungszeugnisse (Criminal Records Bureau) gab bekannt, dass bei ca. 2.700 Personen fälschlicherweise Vorstrafen notiert wurden und einige aufgrund dieser Fehlinformationen keine Stelle bekamen⁶⁸. Schätzungen zufolge wird einer von sechs Briten den von der Regierung beantragten ID-Ausweis aufgrund technischer Probleme nicht nutzen können.⁶⁹

Dieses technische Versagen könnte den Zugang zu bestimmten Orten oder den Zugriff auf Dienstleistungen einschränken. In anderen Fällen, z.B. in der medizinischen Überwachung, könnte es jedoch lebensbedrohlich sein – und kommt viel häufiger vor, als es den meisten Menschen bewusst ist.

Technisches Versagen oder Unzulänglichkeit könnten daher auf so manches Leben schlimmere Auswirkungen haben als ein erfolgreich eingeführtes System.

Die Konsequenzen einer Überwachungsgesellschaft

Die Überwachungsgesellschaft bietet uns Vorteile und Rechte, hat jedoch auch negative – z.T. große und potenziell nicht rückgängig zu machende – Konsequenzen. Jede öffentliche Debatte zu diesem Thema muss auch die Auswirkungen auf die Privatsphäre, ethische und menschenrechtliche Aspekte, den Einfluss auf gesellschaftliche Ein- bzw. Ausgrenzung, Veränderungen der Wahlmöglichkeiten sowie Macht- und Ermächtigungsgefüge untersuchen und gleichzeitig hinterfragen, ob die Betreiber dieser Systeme zur Verantwortung gezogen werden können und ob die Überwachungsverfahren transparent genug sind.

Privatsphäre, Ethik, Menschenrechte

Bei vielen aktuellen Überwachungsdebatten geht es um die „Privatsphäre“. Seit 1970 wurden in Europa und andernorts viele Datenschutzgesetze eingeführt. Dennoch war es recht schwierig, die Politiker auch von den tieferen *gesellschaftlichen* Dimensionen des Datenschutzes⁷⁰ zu überzeugen, ganz zu schweigen von anderen, nicht mit der Privatsphäre verbundenen Problemen einer Überwachungsgesellschaft. In vielen Fällen sind sich die Menschen eines Unrechts gar nicht bewusst und haben daher auch keine Möglichkeit, es zu identifizieren, sich an kompetenter Stelle darüber zu beschweren und entsprechende Rechtshilfen zu beantragen.

Der Schutz dieser Privatsphäre ist wichtig, doch die ethischen und menschenrechtlichen Probleme einer Überwachungsgesellschaft gehen weit darüber hinaus.

Man kann von Otto Normalverbraucher nicht erwarten, dass er sich selbst schützt. Dabei treten die drei folgenden Kernprobleme auf:

Gesellschaftliche Ausgrenzung, Diskriminierung

Wie im vollständigen Bericht dargelegt wird, unterscheidet sich die Überwachung je nach Standort und Gesellschaftsschicht, ethnischer Zugehörigkeit und Geschlecht. Überwachung, Eingriffe in die Privatsphäre und Datenschutz unterscheiden sich je nach Gruppe, bieten Vorteile für einen Gesellschaftsteil und Nachteile für einen anderen. Die Überwachung ist im Einklang mit Änderungen im Gesundheits- und Wohlfahrtssystem gewachsen, in vielen Fällen wurden staatliche Dienstleistungen auf ein simples Risikomanagement reduziert, das umfassende Kenntnis der jeweiligen Sachlage verlangt. Die Erfassung von Personendaten ist damit eine Grundvoraussetzung für die Verteilung der Ressourcen.⁷¹ Und da die Überwachungsnetze so umfassend miteinander

verbunden sind, können Versicherungsgesellschaften wesentlich einfacher mit der Polizei und Supermärkte mit Datenerfassungsunternehmen zusammenarbeiten. Das Ergebnis? Polizeiliche Brennpunkte finden sich hauptsächlich in nicht-weißen Gebieten und große Supermärkte siedeln sich in gehobenen Wohnvierteln oder Vororten an, die sich eher mit dem Auto erreichen lassen.

Die gesellschaftliche Endlösung?

Die Wohngebiete des Jahres 2016 unterteilen sich sehr viel deutlicher in umzäunte Privatgemeinschaften (wie die der Familie Jones), die von gut ausgestatteten Wach- und Schließgesellschaften patrouilliert werden, und in ehemalige Wohnsiedlungen bzw. billige Sozialwohnungen wie die Dobcroft Estate auf. Die Kamera- und Identifikationssysteme in und um ihre feine Wohngegend reduzieren die Versicherungskosten der Familie Jones auf ein Minimum⁷². In der Siedlung Dobcroft Estate wurde Yasmins Arbeit in einem von mehreren Behörden gestellten Sozialarbeiterteam inzwischen an eine private Arbeitsgemeinschaft mit dem optimistischen Namen „Total Social Solutions“ outgesourct. TSS soll die persönlichen Verhaltensprogramme („Personal Behaviour Schemes“ – PBS⁷³) überwachen und durchsetzen, denen jeder Dobcroft-Bewohner von Geburt an⁷⁴ (und in einigen Fällen sogar früher⁷⁵) „beitritt“. Viele der Bewohner mit umfangreichem PBS, z.B. einer Bewährungsstrafe⁷⁶, lassen sich aktive RFID-Chips implantieren, die automatisch mit Sensoren in ihren Wohnungen und am Eingang der Siedlung verbunden sind⁷⁷. Offiziell kann sich jeder freiwillig für oder gegen einen RFID-Chip entscheiden, doch genau wie bei den Überwachungsprogrammen in Läden und Schulen bringt eine Kooperation Vorteile mit sich, nicht zuletzt eine vorzeitige Aufhebung der Bewährung. Gegenwärtig unterliegt die gesamte Dobcroft-Siedlung einer der regelmäßig verhängten Ausgangssperre, da eine ältere Frau aus der Seniorenresidenz Sunnyview „Jugendliche“ aus der Siedlung erkannt haben will, die Ärger machten. Die Frau entdeckte die verdächtigen Aktivitäten auf einer der örtlichen Videokameras, die über Digitalfernsehen auf dem lokalen Sicherheitssender beobachtet werden können. Der Fernseher bringt gleichzeitig eine „Rowdy-Galerie“ all jener ins Wohnzimmer, die bekanntermaßen gegen ihr PBS⁷⁸ verstoßen haben. Zwischen 18.00 Uhr abends und 6.00 Uhr morgens darf derzeit kein Jugendlicher unter 18 Jahren die Siedlung betreten oder verlassen.

Wahlfreiheit, Macht und Ermächtigung

Welches Mitspracherecht haben wir bei der Einführung der Überwachungsgesellschaft? Normale Bürger können und werden Änderungen bewirken – vor allem, wenn sie auf die Einhaltung vorgegebener Richtlinien und Gesetze pochen, das System hinterfragen oder ihre Daten nicht zu ungenauen oder zweifelhaften Zwecken hergeben.

Wie weit aber kann eine Einzelperson oder Gruppe ihre individuelle Überwachung kontrollieren und die Erfassung bzw. Nutzung derartiger Personendaten einschränken? Für Laien sind die Überwachungssysteme häufig technisch viel zu ausgereift, sie verschwinden in den Alltagsstrukturen und -systemen unserer Gesellschaft: am Arbeitsplatz, in der Freizeit, zu Hause, in der Schule, auf Reisen, in der Kommunikation oder im öffentlichen Dienst. Da scheint es sehr viel schwieriger, den kleinen Unterschied zu bewirken. Das Ausmaß persönlicher Profilerstellung durch Großkonzerne⁷⁹ wird vielen Verbrauchern z.B. erst dann klar, wenn ein Identitätsdiebstahl in den Medien publik gemacht wird. Und selbst in so einem Fall scheint sich alles um Sicherheit und Vorbeugung gegen ähnlich betrügerische Aktivitäten zu drehen. Dass die Macht großer Konzerne bzw. staatlicher Behörden über individuelle Daten eingeschränkt werden sollte, wird kaum erwähnt. Wenn es um die Auswirkungen der Überwachung auf ihr Leben geht, sind Einzelpersonen deutlich im Nachteil.

Transparenz, Verantwortlichkeit

Die Infrastrukturen der Wirtschaft, des Transportwesens und der Regierung verfügen über Überwachungskapazitäten, die rapide ansteigen. Einzelne Personen und Gruppen hingegen können kaum feststellen, was eigentlich mit ihren Personendaten passiert oder wem sie wann und zu

welchem Zweck in die Hände geraten. Schritt für Schritt verändern genau diese Personendaten unsere Lebenschancen und lenken unsere Wahlmöglichkeiten. Die zuständigen Organisationen müssen hier zur Verantwortung gezogen werden – vor allem dann, wenn eine intensive Überwachung routinemäßig und mit potenziellen Folgeschäden durchgeführt wird. Zusätzlich zu den Aufgaben der Aufsichtsbehörden, d.h. der aktiven Kontrolle und Druckausübung in Richtung minimaler Überwachung, muss ein Wandel vom Selbstschutz gegen Datenmissbrauch hin zur Verantwortlichkeit der Datensammler erfolgen.

Die Herausforderung für Aufsichtsbehörden

Ist es überhaupt möglich, die Überwachung zu überwachen? Ihre negativen Auswirkungen unter Kontrolle zu halten und sie mit der von uns gewünschten Gesellschaft und Demokratie in Einklang zu bringen?⁸⁰ Studien, die die Auswirkungen neuer Projekte auf Privatsphäre und Überwachung untersuchen, würden das öffentliche Bewusstsein steigern, die öffentliche Debatte anregen und den Aufsichtsmechanismen eine weitere wichtige Dimension verleihen. Der Datenschutz unterliegt vielen Gesetzen und Verhaltenskodexen. Auch bestimmte Technologien dienen dem Schutz persönlicher Daten. Spezielle Aufsichtsbehörden forcieren die Umsetzung der Gesetze, unterstützen individuelle Beschwerden oder versuchen, auf die Politik der Regierung bzw. wirtschaftliche Entwicklungen Einfluss zu nehmen. Bürgerinitiativen und die Medien machen uns auf die Gefahren der Überwachung aufmerksam. Doch die Macht und Effektivität dieser Aufsichtsmechanismen muss in Frage gestellt werden: Sie sollten überdacht und verbessert werden. Denn der Datenschutz ist nur ein Teil des Problems, nicht aber das gesamte Problem. Mehr Menschen müssen das Thema Überwachung verstehen und an Entscheidungen beteiligt werden, die ggf. zu Taten führen und die Überwachung in den Dienst des Menschen stellen. Diese Kontrollen dürfen allerdings nicht nur isoliert in einem Land bzw. einer Ländergruppe wie der EU durchgeführt werden. Die Informationen im Räderwerk der Überwachung fließen um die ganze Welt – ebenso wie die Bewegungen und Aktivitäten, die überwacht werden. Um sich diesen Herausforderungen zu stellen, ist eine rundum integrierte, globale Aufsicht erforderlich.

Das Leben – ein Spiegelsaal

Im Jahr 2016 wird jeder überwacht. Doch die Menschen, vor allem gut ausgebildete oder wohlhabende, sind sich dieser Überwachung zunehmend bewusst und finden neue Möglichkeiten, sie zu handhaben. Gareth Jones nutzt einen Managementservice für Personendaten, der seinen „Online-Datenschatten“ überwacht, falsche Informationen in Regierungs- und Verbraucherdatenbanken automatisch korrigiert und ihn auf andere Probleme aufmerksam macht. Sein teurer Handheld ist in der Lage, Einzelhandelswerbung einfach zu blockieren. Leider kann nicht jeder so einfach auf persönliche Daten zugreifen und sie ändern. Alle, die sich mit dem Management ihrer Personendaten nicht so gut auskennen oder kein Geld für einen entsprechenden Service haben, sind deutlich im Nachteil. Nach Protestkampagnen lassen sich vom Staat oder von Privatgesellschaften gespeicherte Personendaten leichter einsehen und ändern, aber nur, wenn die entsprechende Person einen ID-Ausweis hat. Ein ID-Ausweis ist im Übrigen auch Voraussetzung für viele andere Dinge im Leben.

Das Verhältnis zwischen Bürger und Staat hinsichtlich des Eigentums dieser Daten und des Rechts auf ihre Änderung (Stichwort „gläserner Bürger“) ist deutlich gespannt und verursacht bisher noch ungelöste Probleme. Im Jahre 2016 haben sich die Menschen jedoch an die Überwachung von anderen und durch andere gewöhnt. Viele führen freiwillig eine persönliche Lebensüberwachung (Life-logging) durch, die sie archivieren oder in einer Art öffentlichem Online-Tagebuch in Echtzeit ins Internet stellen.⁸¹ Hardliner führen Überwachung in Selbstjustiz durch, da sie von den „weichen Regierungsmaßnahmen“ gegen Terrorismus, Kriminalität und illegale Einwanderung⁸² enttäuscht sind. Inoffizielle Webseiten mit „mutmaßlichen Tätern“ wuchern im Internet und führen zu vielen Irrtümern und Fehlidentifikationen.⁸³ Gegner, Künstler und Surrealisten spielen auf vielerlei Art und Weise mit der allgegenwärtigen Überwachung und setzen sich so gegen sie zur Wehr. Sie schalten z.B. öffentliche Überwachungsgeräte ab⁸⁴ oder nutzen sogenannte „Unterwachungstechnologie“ („Sousveillance“), die die Überwachung ausgleicht oder ausschaltet⁸⁵. Antikapitalisten wie Aaron und Ben verbringen ihre Samstage vorzugsweise damit, selbstklebende Aluminiumbleche und batteriebetriebene Mini-Mikrowellensender an Ladeneingängen anzubringen, die die kabellose Kommunikation unterbrechen.⁸⁶ Aber auch das Life-logging ist noch nicht das Nonplusultra, denn dank immer ausgereifterem Datenmanagement und Videosoftware lässt sich jedes Leben anpassen oder völlig neu kreieren – sei es nun zu reinen Unterhaltungszwecken oder aus umstürzlerischen oder betrügerischen Beweggründen. Im Jahr 2016 existiert eine zunehmende Masse an virtuellen Datenschatten, für die es in der Realität kein entsprechendes Pendant mehr gibt, die dahinzuleben scheinen und selbst einem Informationsmanagement unterworfen sind. Auch sie werden von automatischen Systemen, die leise und unsichtbar agieren, online überwacht – ein Heer virtueller Bewohner eines endlosen Spiegelsaals ...

Quellenangaben

Hinweis: Alle Webseiten waren zum 1. September 2006 abrufbar.

¹ Dieser Blick in eine mögliche Zukunft stammt aus Teil C des Gesamtberichts, der auch den vollständigen „Wochenbericht“ einer typischen Familie aus dem Jahre 2006 enthält.

² UAVs werden schon seit Jahren vom amerikanischen Militär eingesetzt: Das beste Beispiel ist derzeit die unbemannte Drohne „Predator“, die im Irak eingesetzt wird, siehe: „Predator RQ-1 / MQ-1 / MQ-9 Unmanned Aerial Vehicle (UAV), USA“, *airforce-technology.com*, 2006, <http://www.airforce-technology.com/projects/predator/>. Für Großbritannien wurden viele Einsatzmöglichkeiten vorgeschlagen, siehe: Jha, A., „On the horizon ... pilotless planes as fishermen's and firefighters' friends“, *The Guardian*, 30. August 2006, <http://www.guardian.co.uk/science/story/0,1860825,00.html>. In Los Angeles experimentiert die Polizei bereits mit kleinen, ferngesteuerten Spionageflugzeugen namens „SkySeer“: Bowes, P., „High hopes for drone in LA skies“, *BBC News*, 6. Juni 2006, <http://news.bbc.co.uk/1/hi/world/americas/5051142.stm>.

³ Große Sportveranstaltungen werden gern als Test- und Implementierungsterrain für neue Überwachungstechnologien eingesetzt, z.B. die CCTV-Überwachung während der Weltmeisterschaft in Japan 2002, siehe: Abe, K., (2004) „Everyday policing in Japan: surveillance, media, government and public opinion“, *International Sociology*, 19, 215–231; oder die CCTV-Überwachung während der Olympiade in Athen, siehe: Samatas, M. (2004) *Surveillance in Greece*, Athens: Pella.

⁴ Siehe „Crime and Justice and Infrastructure Expert Reports“. Eines der größten Probleme bei der Gesichtserkennung ist der Blickwinkel der CCTV-Kameras; siehe z.B.: Introna, L. und Wood, D. (2004) „Picturing algorithmic surveillance: the politics of facial recognition systems“, *Surveillance & Society*, 2(2/3): 177-198.

⁵ Die Kontrolle städtischer Bereiche wird zunehmen an PPPs (Public-Private Partnerships) und innerstädtische Managementorganisationen (<http://www.atcm.org/>) sowie BIDs übergeben. Nach Ansicht der Regierung stellen die BIDs „eine Investition in den örtliche Handel dar, weil sie wertschöpfende Dienstleistungen stellen“: <http://www.ukbids.org/>. Eines der größten Aufsichtsprobleme des Jahres 2016 bezieht sich auf die Informationsübertragung zwischen staatlichen und privaten Wach- und Schließgesellschaften, die im Auftrag oder anstatt des Staates agieren, und dies in einer Zeit, in der ein Police National Computer (PNC) viele Datenbanken verlinkt und die Polizei, Bewährungshelfer, Gefängnis- und Sozialdienste miteinander verbunden sind.

⁶ Viele Polizeidienste testen diese bereits, siehe z.B.: „Pocket computers put police 'in the picture““, *West Yorkshire Police*, 28. März 2006, <http://www.westyorkshire.police.uk/section-item.asp?sid=12&iid=2226>; auch das „Airwave-Programm“ (siehe „Crime and Justice Expert Report“) integriert sie bereits.

⁷ Auch Helmkameras, die live mit der Einsatzzentrale verbunden sind, werden vielerorts schon eingeführt, siehe z.B.: „Police use anti-yob head cameras“, *BBC News*, 23. März 2006, http://news.bbc.co.uk/1/hi/wales/north_east/4836598.stm.

⁸ Im Jahre 2016 haben die Polizei und ihre Verbündeten im Privatsektor nahezu alle Datenbanken mit dem PNC vernetzt.

⁹ Auch im Jahre 2016 richten sich Medien und Politik gegen diese Polizeimethode. Es wird jedoch argumentiert, dass ID-Ausweise die guten Absichten einer Person demonstrieren und man nicht grundsätzlich von der Unschuld einer Person ohne ID-Ausweis ausgehen kann.

¹⁰ Ford, R., „Beware rise of Big Brother state, warns data watchdog“, *The Times*, 16. August 2004, http://www.timesonline.co.uk/article/0,,2-1218615_1,00.html.

¹¹ Die vollständigen Auswirkungen einer Überwachung auf den Alltag der Menschen wird in Teil C des Gesamtberichts dargestellt.

¹² Die Zahlen stammen von *SecurityStockWatch.com 100 Index*, August 2006: <http://www.securitystockwatch.com/>.

¹³ Siehe z.B.: „The future of screening“, *BBC News*, 14. Dezember 2002, <http://news.bbc.co.uk/1/hi/health/2570787.stm>.

¹⁴ McKie, R., „Icelandic DNA project hit by privacy storm“, *The Observer*, 16. Mai 2004, <http://observer.guardian.co.uk/international/story/0,6903,1217842,00.html>. Rose, H. (2001) *The Commodification of Bioinformation: The Icelandic Health Sector Database*, London: The Wellcome Trust.

¹⁵ Dies wird in Lyon, D. *Surveillance after September 11*, Cambridge, UK: Polity Press, 45–48, 142ff, diskutiert.

¹⁶ Garton Ash, T. (1997) *The File: A Personal History*, New York: Vintage.

¹⁷ Bargeldgeschäfte können normalerweise zwar nicht direkt mit dem Verbraucher in Verbindung gebracht werden, dienen aber häufig dem Vergleich mit ähnlichen Transaktionen in der Vergangenheit und der Analyse von Verbrauchertypen, die ähnliche Einkäufe getätigt haben.

¹⁸ Siehe Fink, J. und Kosba, A. (2000) „A review and analysis of commercial user modeling servers for personalization on the world wide web“, *User Modeling and User-Adapted Interaction*, 10, 209–249.

¹⁹ The Wanless Report (2002) *Securing Our Future Health: Taking a Long-Term View: Final Report*, London: HM Treasury.

²⁰ PITO (2005) *Police Information Technology Organisation, Annual Report 2004 – 2005*, HC 261, London: The Stationery Office.

²¹ Randerson, J., „DNA of 37% of black men held by police“, *The Guardian*, 5. Januar 2006, <http://www.guardian.co.uk/frontpage/story/0,,1678168,00.html>.

²² PITO (2006) *Facial Images National Database (FIND)*, <http://www.pito.org.uk/products/FIND.php>.

²³ ACPO (Association of Chief Police Officers) (2002) *Infinet: A National Strategy for Mobile Information*, Association of Chief Police Officers.

²⁴ Inoffizielle Rassenprofile gibt es zweifellos bereits, und das seit langer Zeit. Die britische Polizei hat diese Vorgehensweise auch offiziell vorgeschlagen, siehe: „No racial profiling by anti-terror police, says minister“ *Times Online*, 2. August 2005, <http://www.timesonline.co.uk/article/0,,22989-1717624,00.html>.

Hintergründe, siehe: „Racial Profiling: Old and New“, *ACLU*, <http://www.aclu.org/racialjustice/racialprofiling/index.html>.

²⁵ Siehe „Borders Expert Report“.

²⁶ Die Internationale Zivile Luftfahrtbehörde (International Civil Aviation Authority) hat 2004 Normen für maschinenlesbare Reisedokumente (Machine Readable Travel Documents – MRTD) vereinbart. Dieser Prozess wurde von der Initiative der G8-Länder für sicheren und problemlosen internationalen Reiseverkehr (Secure and Facilitated International Travel Initiative – SAFTI) vorangetrieben: „G8 meeting at Sea Island in Georgia, USA - sets new security objectives for travel“, *Statewatch*, 2004, <http://www.statewatch.org/news/2004/jun/09g8-bio-docs.htm>.

Dies gilt trotz der Bedenken gegen ein leichtes Klonen von RFID-Chips: Johnson, B., „Hackers crack new biometric passports“, *The Guardian*, 7. August 2006,

<http://politics.guardian.co.uk/homeaffairs/story/0,,1838754,00.html>. Die Tatsache, dass sich britische ID-Ausweise leicht in biometrische Pässe verwandeln oder mit diesen verschmolzen werden können, wurde bereits notiert: Lettice, J., „UK biometric ID card morphs into £30 'passport lite““, *The Register*, 8. Juli 2005, http://www.theregister.co.uk/2005/07/08/id_card_as_passport/.

²⁷ Siehe „Consumer Expert Report“. Im Jahr 2016 gibt es weiterhin Streitfragen zwischen den Staaten und der outgesourceten Grenzüberwachung hinsichtlich des Eigentums von Reisedaten. Die britische Regierung hält an ihrem „Recht“ fest, ID-Daten, wie 2006 vorgeschlagen, zu verkaufen: Elliot, F., „ID plans: powers set to widen“, *The Independent*, 6. August 2006, <http://news.independent.co.uk/uk/politics/article1216000.ece>. Die einzige Stimme, die hier nicht gehört wird, ist die des Bürgers.

²⁸ Diese Ganzkörper-Scanner gibt es in verschiedenen Ausführungen, die bereits in der Praxis getestet werden, so z.B. der niedrig dosierte Röntgenapparat Secure 1000 von Rapiscan:

<http://www.rapiscansystems.com/sec1000.html>, getestet auf dem Flughafen Heathrow, siehe: Lettice, J., „See through clothes' scanner gets outing at Heathrow“, *The Register*, 8. November 2004,

http://www.theregister.co.uk/2004/11/08/heathrow_scanner_pilot/, oder der mm-Wellen-Scanner, der von QinetiQ entwickelt und von Eurotunnel getestet wurde: http://www.qinetiq.com/home/newsroom/news_releases_homepage/2004/3rd_quarter/Next_generation_security_screening.html.

²⁹ Campbell, D. (1999) *Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control)* Band 2/5: *The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition (AKA Interception Capabilities 2000)*, Luxemburg: Europa-Parlament, Generaldirektorat Forschung, Direktorat A, STOA-Programm.

³⁰ Im Jahr 2016 haben die meisten Menschen so ein Gerät, das kabellosen Internet-Zugriff über Roaming, Telefondienste, Computernavigation u.v.a.m. zulässt. Die Navigationsfunktion stellt außerdem sicher, dass der Standort der Geräte (und damit ihrer Bediener) jederzeit festgestellt werden kann.

³¹ Galileo ist die zivile Antwort Europas auf das amerikanische Militärsystem GPS. Der erste Satellit erreichte seine Umlaufbahn im Jahre 2004, ab 2008 werden die ersten Dienstleistungen zur Verfügung stehen. Siehe: „Galileo, European Satellite Navigation System“ EG-Kommission Direktorat allg. Energie und Verkehr, http://ec.europa.eu/dgs/energy_transport/galileo/intro/future_en.htm.

³² Das britische Gesetz über Ermittlungsbefugnisse (Regulation of Investigatory Powers – RIP) erlaubt nur eine begrenzte Speicherung der Aufzeichnungen. Man kann jedoch davon ausgehen, dass Polizei und Sicherheitsdienste bis zum Jahr 2016 alle offenen „Gesetzeslücken“ schließen werden – höchstwahrscheinlich als Antwort auf einen in den Medien breitgetretenen Skandal, der sich auf Terrorismus oder Kindesmissbrauch bezieht.

³³ Cracking bezieht sich auf „Aktivitäten, durch die in ein Computersystem eingebrochen werden kann“, *The New Hacker's Dictionary*, http://www.outpost9.com/reference/jargon/jargon_toc.html.

³⁴ MMOGs verfügen gegenwärtig laut Schätzungen über ca. 13 Millionen Teilnehmer, die Mehrzahl in der *World Of Warcraft*, <http://www.worldofwarcraft.com/index.xml>, sowie in der koreanischen Spielfamilie *Lineage I*, <http://www.lineage.com/>, und *II*, <http://www.lineage2.com/>. Andere virtuelle Welten stellen sich eher als analoge Kopien der Realität dar, so z.B. *Second Life*: <http://secondlife.com>. Sie dringen immer weiter vor, ihre Wirtschaftsgefüge überschneiden sich zunehmend mit der realen Welt, in der Gegenstände aus den Spielen gegen „echtes“ Geld versteigert werden, so z.B. auf *ebay*, <http://www.ebay.com>. Statistische Analysen entnehmen Sie bitte *MMOGCHART.COM*, <http://www.mmogchart.com/>.

³⁵ Über „virtuelle Überwachung“ wurde bereits berichtet, siehe z.B.: „Confessions of a Virtual Intelligence Analyst“, *Terranova*, 15. März 2006, http://terranova.blogs.com/terra_nova/2006/03/confessions_of_.html. Marketinganalysten haben bedeutende aufstrebende, aber virtuelle Märkte entdeckt, d.h. die Unternehmen richten ihren Fokus zunehmend auf Spielwelten, siehe z.B.: Burns, E., „Marketing Opportunities Emerge in Online Gaming Venues“, *ClickZ*, 1. August 2006, <http://www.clickz.com/showPage.html?page=3623035>, die ersten „virtuellen Reklamewände“ gibt es auch schon, siehe: Shields, M., „Massive Unveils Toyota Ad Units Within Anarchy“, *Mediaweek*, 19. Juli 2006, http://www.mediaweek.com/mw/news/interactive/article_display.jsp?vnu_content_id=1002876380.

³⁶ Dies erfolgte im Anschluss an eine Reihe von MMOG-Vorfällen im Lauf mehrerer Jahre, die in die Wirklichkeit übertragen wurden; siehe z.B.: „Chinese gamer sentenced to life“, *BBC News*, 8. Juni 2005, <http://news.bbc.co.uk/1/hi/technology/4072704.stm>.

³⁷ McCahill, M. und Norris, C. (2003), „Estimating the Extent, Sophistication and Legality of CCTV in London“, in M. Gill (Red.) *CCTV*, Leicester: Perpetuity Press.

³⁸ Norris, C. und Armstrong, G. (1999) *The Maximum Surveillance Society: The Rise of Closed Circuit Television*, Oxford: Berg, 42.

³⁹ Norris, C. (2006) „Closed Circuit Television: a review of its development and its implications for privacy“, ein Referat für die Quartalsversammlung des *Department of Home Land Security Data Privacy and Integrity Advisory Committee* vom 7. Juni in San Francisco, Kalifornien.

⁴⁰ Gill, M. und A. Spriggs (2005) *Assessing the Impact of CCTV*. London: Home Office Research, Development and Statistics Directorate, 43, 60–61.

⁴¹ Wilkins, G. und Additcott, C. (1998) *Motoring Offences England and Wales 1996*, Home Office Statistical Bulletin, London: Home Office; Ransford, F., Perry, D., Murray, L. (2005) *Motoring Offences and Breath Test Statistics: England and Wales 2003*, Home Office Statistical Bulletin, London: Home Office.

⁴² McCahill und Norris, 2003, *op cit*.

⁴³ PA Consulting (2004) *Denying Criminals the Use of the Road*, http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ANPR_10,000_Arrests.pdf?view=Binary.

⁴⁴ *ibid.*: 6.

⁴⁵ *ibid.*: 18.

⁴⁶ Es gibt viele potenzielle Programme, siehe z.B.: Independent Transport Commission (2006) *Paying to Drive*, http://trgl.civil.soton.ac.uk/itc/p2d_main.pdf.

⁴⁷ Der Nachteil ist hier, dass eine Organisation nur einen bestimmten Personentyp einstellen und daher über eine weniger vielseitige Belegschaft verfügen würde – siehe „Workplace Surveillance Expert Report“.

⁴⁸ NPS (2006a) – National Probation Service – *Electronic Monitoring*: 6.

<http://www.probation.homeoffice.gov.uk/output/Page137.asp#Current%20Programmes>.

⁴⁹ Das HDC-Programm ermöglicht Verurteilten mit einer Gefängnisstrafe von drei Monaten bis maximal vier Jahren eine frühzeitige Entlassung für einen Zeitraum zwischen zwei Wochen und 4½ Monaten.

Voraussetzung ist jedoch eine Ausgangssperre, die über elektronische Fußfesseln kontrolliert wird. Im Zeitraum 2004/5 wurden 19.096 Personen im Rahmen dieses Programms frühzeitig entlassen. (NPS, *op cit.*:6).

⁵⁰ NPS, *op cit*.

⁵¹ Einzelheiten, siehe PETS-Webseite des Department of Environment, Food and Rural Affairs (DEFRA): <http://www.defra.gov.uk/animalh/quarantine/pets/index.htm>.

⁵² Bei diesem Unternehmen handelt es sich um die Verichip Corporation: <http://www.verichipcorp.com/>.

- ⁵³ Amal Graafstra ist ein bekannter Enthusiast und Verfechter des „Self-Chipping“. Erläuterungen, Bilder und Videos können von seiner Webseite heruntergeladen werden: <http://amal.net/rfid.html>.
- ⁵⁴ Graham-Rowe, D., „Clubbers chose chip implants to jump queues“, *New Scientist*, 21. Mai 2004, <http://www.newscientist.com/article.ns?id=dn5022>.
- ⁵⁵ Waters, R., „US group implants electronic tags in workers“, *Financial Times*, 12. Februar 2006, <http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html>.
- ⁵⁶ Der britische Design Council definiert den Ursprung des Begriffs „Brandscape“ als „gesamte Erfahrungsreichweite und Nutzung einer Marke. Dieser Begriff umfasst alle Personen, die mit dieser Marke in Verbindung stehen und mit ihr interagieren, darunter auch Kunden, Lieferanten, Mitarbeiter, Wettbewerber, Fachhändler, Vertriebsgesellschaften, Partner usw.“: http://www.design-council.org.uk/webdav/harmonise?Page/@id=6046&Session/@id=D_rPJLjJbFNakH0E0GQvlo&Document%5B@id%3D5232%5D/Chapter/@id=7.
- ⁵⁷ Die „wertvollsten“ Kunden werden über eine Kreditprüfung und ihr Verbraucherprofil ermittelt. Als wertvoller Kunde gibt man wahrscheinlich mehr Geld aus. Implantate entwickeln sich somit zum Statussymbol.
- ⁵⁸ Siehe Baja Beach (nd.) ‘Zona VIP’, <http://www.bajabeach.es/>.
- ⁵⁹ Auf diese Weise werden der Datenbank weitere Informationen über die Bedürfnisse und Wünsche einer Person zugeführt.
- ⁶⁰ Siehe „Oyster data use rises in crime clampdown“, *The Guardian*, 13. März 2006, <http://politics.guardian.co.uk/foi/story/0,,1730771,00.html>.
- ⁶¹ Siehe die klassische Studie von Oscar Gandy, *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, Colorado: Westview, 1993.
- ⁶² In den USA steckt dieses Verfahren derzeit in den Kinderschuhen. Siehe z.B. Leff, L. „Students ordered to wear tracking tags“, *Associated Press*, 9. Februar 2005, <http://www.msnbc.msn.com/id/6942751/>.
- ⁶³ Siehe z.B.: „Neglect ruling in girl pond death“, *BBC News*, 23. März 2006, http://news.bbc.co.uk/1/hi/england/coventry_warwickshire/4837614.stm.
- ⁶⁴ In Großbritannien werden Schulen je nach den Prüfungsergebnissen ihrer Schüler in eine Rangliste aufgenommen.
- ⁶⁵ Z.B. Nestlé, Unilever, Pepsico usw.
- ⁶⁶ United States Visitor and Immigrant Status Indicator Technology – gibt es seit 2004 in allen Inlands-, Flug- und Seehäfen.
- ⁶⁷ Siehe: Amoore, L. (2006) „Biometric Borders: Governing Mobilities in the War on Terror“, *Political Geography* 25(2): 336-351.
- ⁶⁸ „Criminal records mix-up uncovered“, *BBC News*, 21. Mai 2006, <http://news.bbc.co.uk/1/hi/uk/5001624.stm>.
- ⁶⁹ Siehe: Grayling, A. C. (2005) *In Freedom’s Name: The Case against Identity Cards*, London: Liberty.
- ⁷⁰ Siehe die ausgezeichneten Ausführungen zur Sozialität des Datenschutzes in: Regan, P. (1995) *Legislating Privacy*, Chapel Hill: University of North Carolina Press.
- ⁷¹ Siehe: Ericson, R. und Haggerty, K. (1997) *Policing the Risk Society*, Toronto: University of Toronto Press.
- ⁷² Der Verband britischer Versicherungsgesellschaften (Association of British Insurers – ABI) hat diese Maßnahmen in einem umfangreichen Bericht zum Wohnungswesen gefordert: ABI (n.d.) *Securing the Nation: The Case for Safer Homes*, London: ABI, 12. <http://www.abi.org.uk/BookShop/ResearchReports/Securing%20the%20Nation%20July%202006.pdf>.
- ⁷³ Es wird hier davon ausgegangen, dass Verwarnungen gegen asoziales Verhalten, intensive Überwachungsprogramme u.ä. (siehe „Crime and Justice Expert Report“) für alle, deren Verhaltensmuster auf zukünftige Straftaten schließen lässt, in allgemeinen persönlichen Verhaltensprogrammen (Personal Behaviour Schemes – PBS) zusammengefasst werden. Da alle Bewohner der Dobcroft Estate allein durch ihren Wohnort in einer Siedlung mit kriminellen Tendenzen schon ein Kriterium erfüllen, unterliegen alle einem PBS.
- ⁷⁴ Die sogenannte „Biokriminologie“ oder genetische Untersuchung kriminellen Verhaltens erlebt derzeit eine neue Blüte; siehe z.B.: Rose, D. (2006) „Lives of crime“, *Prospect* 125 (August), http://www.prospect-magazine.co.uk/article_details.php?id=7604. Eine frühere Kritik an diesem Ansatz findet sich in: Rose, N. (2000) „The biology of culpability: pathological identity and crime control in a biological culture“, *Theoretical Criminology*, 4 (1), 5–34.
- ⁷⁵ Der wachsende Enthusiasmus für eine noch frühere Intervention bezieht sich nun bereits auf diese erste Lebensphase, siehe z.B.: Woolf, M., „‘Failures’ targeted at birth“, *The Independent*, 16. Juli 2006, <http://news.independent.co.uk/uk/politics/article1180225.ece>.

⁷⁶ Im Jahr 2016 ist das Gefängnis nur eine weitere Stufe in einem PBS. Sozialarbeit, Bewährungshilfe und Gefängnis gehen nahtlos ineinander über und liegen größtenteils in privater Hand.

⁷⁷ Aus „Sicherheitsgründen“ wurde die Dobcroft Estate im Jahr 2010 eingezäunt. Die vier verbleibenden Ein- und Ausgänge werden von Community Support Officers, Kameras und RFID-Scannern bewacht.

⁷⁸ Mit einem derartigen Programm wurde 2006 im Londoner Stadtteil Shoreditch experimentiert. Es wurde sofort als „ASBO-TV“ (etwa: Asozialen-TV) bezeichnet, siehe z.B.: Swinford, S., „Asbo TV helps residents watch out“, *Times Online*, 8. Januar 2006, <http://www.timesonline.co.uk/article/0,,2087-1974974,00.html>.

⁷⁹ Siehe Leitartikel der *New York Times*: „The data-fleeing of America“, 21. Juni 2005.

⁸⁰ Siehe Bennett, C. und Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective*, 2. Ausgabe, Cambridge, MA: MIT Press.

⁸¹ „Life-logging“ entwickelte sich aus dem Web-logging. Inzwischen wird dieses Phänomen von den verschiedensten Technologien unterstützt; siehe z.B.: Ward, M. „Log your life via your phone“, *BBC News*, 10. März 2004, <http://news.bbc.co.uk/1/hi/technology/3497596.stm>.

⁸² Siehe „Borders Expert Report“ und z.B. die selbsternannten US-Grenzschrützer „Minutemen“: <http://www.minutemanproject.com/>.

⁸³ Dies wurde bereits in Verbindung mit einem Fall von Kindesmissbrauch zur Kenntnis genommen, bei der eine Kinderärztin im Jahr 2000 aus ihrem Haus vertrieben wurde, siehe z.B.: Allison, R., „Doctor driven out of home by vigilantes“, *The Guardian*, 30. August 2000, <http://www.guardian.co.uk/child/story/0,7369,361031,00.html>. Wir gehen schlicht davon aus, dass solche Irrtümer mit der Technologie des Jahres 2016 noch schneller und auf noch breiterer Front in Umlauf gesetzt werden können.

⁸⁴ Für einen derartigen Widerstand gibt es bereits viele Ratgeber; siehe z.B.: „Guide to Closed Circuit Television (CCTV) destruction“, *Schnews*, <http://www.schnews.org.uk/diyguide/guidetoclosedcircuittelevisioncctvdestruction.htm>.

⁸⁵ Siehe Mann, S., Nolan, J. und Wellman, B. (2004) „Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments“, *Surveillance & Society*, 1(3), 331–355.

⁸⁶ RFID ist eine Sichtlinientechnologie. Interferenzen lassen sich mit Mikrowellen, Metallblechen, Ziegelsteinen und sogar Baumharz erzielen, siehe z.B.: „RFID Technology“, *RFID Centre*, <http://www.rfidc.com/docs/rfid.htm>.