

Überwachung, Privatsphäre und Sicherheit

Was ist Ihre Meinung?



surprise
surveillance
privacy
security



Inhalt

1 Willkommen zum Projekt SurPRISE	5
1.1 Wie ist diese Broschüre zu lesen?	6
2 Zusammenfassung	7
3 Ein gewöhnlicher Tag...	9
3.1 Überwachung, Privatsphäre und Sicherheit	10
3.1.1 Überwachung	10
3.1.2 Privatsphäre und Datenschutz: Wichtige Aspekte?	11
3.1.3 Sicherheit	12
4 Drei neue Sicherheitstechnologien	13
Was macht eine neue Sicherheitstechnologie mehr oder weniger akzeptabel für Sie?	13
5 Intelligente Videoüberwachung – Smart CCTV	15
5.1 Warum Smart CCTV entwickelt wurde	15
Wie funktioniert Smart CCTV?	16
5.2 Wie Smart CCTV verwendet wird	17
5.3 Verbesserungen im Bezug auf die Sicherheit	18
5.4 Kritische Aspekte	18
6 Cyber-Überwachung durch Deep Packet Inspection	21
6.1 Wozu Deep Packet Inspection entwickelt wurde	21
Wie Deep Packet Inspection funktioniert	22
6.2 Wie Deep Packet Inspection funktioniert	22
6.2.1 Kommerzielle Anwendungen	23
6.2.2 Anwendungen im Bereich der öffentlichen und nationalen Sicherheit	24
6.3 Sicherheitsverbesserungen	24
6.4 Kritische Aspekte	25
7 Smartphone Location Tracking - Handyortung	27
7.1 Warum Smartphone Location Tracking entwickelt wurde	27
Wie Handyortung funktioniert	28
7.2 Wie Smartphone Location Tracking eingesetzt wird	29
7.2.1 Kommerzielle Anwendungen	29
7.2.2 Anwendungen im Bereich öffentliche und nationale Sicherheit	30
7.3 Verbesserungen der Sicherheit	30
7.4 Kritische Aspekte	31
8 Ist Technik die einzige Antwort?	33
8.1 Regionale Lösungen	33
8.2 Nationale oder internationale Lösungen	33
9 Nun zu Ihnen...	35
Über dieses Dokument	36
Projekt-Partner	37

1 Willkommen zum Projekt SurPRISE

SurPRISE ist ein EU-weites Forschungsprojekt zu den Themen Privatsphäre und Sicherheit. SurPRISE steht für die englischen Begriffe „Surveillance“, „Privacy“ und „Security“ (Überwachung, Datenschutz und Sicherheit). Ziel des Projekts ist es, die Meinungen von europäischen BürgerInnen zu neuen Sicherheitstechnologien zu erforschen. Viele dieser Technologien basieren auf der Überwachung von Menschen und deren Aktivitäten. Sie werden von der Polizei oder Sicherheitspersonal eingesetzt, um zu überwachen, was vor sich geht, und um sicherzustellen, dass nichts passiert. Wenn Sie beispielsweise zum Flughafen fahren, wo Ihr Gepäck gescannt wird, oder wenn durch Videoüberwachung (englisch: CCTV – Abkürzung für den Begriff „Closed Circuit Television“) Aktivitäten auf einer Straße, an der sie entlang gehen, aufgezeichnet werden, begegnen Sie überwachungsbasierten Sicherheitstechnologien. Das Ziel von SurPRISE ist es, sicherzustellen, dass diese Technologien effektiv und sicher sind, und die Menschenrechte achten. Um dieses Ziel zu erreichen, benötigen wir Ihre Hilfe.

Wir haben Sie eingeladen, am SurPRISE Projekt teilzunehmen, weil die Europäische Kommission erfahren will, was aus Ihrer Sicht als BürgerIn getan werden sollte, um zu gewährleisten, dass Sie sich geschützt und sicher fühlen. Mit Ihrer Teilnahme am SurPRISE BürgerInnen-Forum können Sie Ihre Meinung zu Sicherheitstechnologien äußern und mit anderen teilen. SurPRISE wird die Ansichten der BürgerInnen erheben und die gewonnenen Erkenntnisse der Europäischen Kommission mitteilen.

Die BürgerInnen-Foren finden in neun europäischen Ländern statt: In Großbritannien, Österreich, Dänemark, Deutschland, Ungarn, Italien, Norwegen, Spanien und der Schweiz. Die Ergebnisse dieser Bürgerbeteiligung werden im Lauf des Jahres 2014 an die Europäische Union übermittelt und Medien, Politik

und öffentlicher Verwaltung sowie BürgerInnen öffentlich zugänglich gemacht.

Diese Broschüre enthält grundlegende Informationen zu jenen Themen, die bei den SurPRISE-Foren diskutiert werden. Sie beinhaltet Informationen über neue Sicherheitstechnologien, die in SurPRISE untersucht werden. Außerdem bietet sie Hintergrundinformationen zu Überwachung, Sicherheit und Datenschutz in Europa.

Wir sind uns bewusst, dass das Lesen dieser Broschüre eine Herausforderung sein kann. Keine Sorge, wir werden nicht den Inhalt abprüfen und es ist auch nicht unser Bestreben, Sie zum Experten in diesen Bereichen zu machen. Das Ziel der Broschüre ist vielmehr, Ihnen eine Vorstellung von den Themen zu vermitteln, die beim BürgerInnen-Forum besprochen werden, damit Sie sich schon vorab Gedanken über Ihre persönlichen Ansichten zu Überwachung, Privatsphäre und Sicherheit machen können. Ihre Teilnahme am Forum ist gerade deshalb so wichtig, weil Sie kein Experte in diesen Bereichen sind. Wir haben Sie für die Teilnahme ausgewählt, weil Sie die europäische Bevölkerung repräsentieren, deren Alltag durch die Entscheidungen von Politikern auf europäischer und nationaler Ebene betroffen ist.

SurPRISE wird EntscheidungsträgerInnen Ihre Meinungen anonymisiert darlegen. Sicherheitstechnologien betreffen Menschenrechte, Fragen nach Gerechtigkeit und Fairness, sowie Vertrauenswürdigkeit und Effektivität von Institutionen. Daher ist es wichtig, dass Debatten die Meinungen der allgemeinen Öffentlichkeit einbeziehen und nicht nur jene von Politik, Industrie, Experten und Hilfsorganisationen. Politiker bestimmen die Sicherheitspolitik, aber Sie als BürgerIn müssen mit den Konsequenzen dieser Entscheidungen leben. Daher ist Ihre Meinung besonders wichtig.

**Wissenschaft informiert.
Sie sagt uns nicht, was zu tun ist.
Die Wahl liegt bei uns allen.
Reden Sie mit, denn Ihre Meinung zählt!**

1.1 Wie ist diese Broschüre zu lesen?

Die Broschüre ist in fünf Abschnitte unterteilt. Der erste Teil besteht aus einer allgemeinen Einführung in die Themen Überwachung, Sicherheit und Datenschutz in Europa. In den darauf folgenden Abschnitten wird auf jene Sicherheitstechnologien eingegangen, die im BürgerInnen-Forum diskutiert werden. Bitte beachten Sie, dass die Broschüre drei ausgewählte Technologien detaillierter beschreibt, jedoch nur zwei davon im Forum behandelt werden. Ihr Einladungsschreiben verrät Ihnen, welche beiden das sind.

Jeder Abschnitt erläutert, warum die Technologie entwickelt wurde, wie sie verwendet wird, welche Erhöhung der Sicherheit sie bietet und wo ihre Grenzen und Probleme liegen. Wir haben eine Info-Box zu jeder Technologie hinzugefügt, die erklärt wie die jeweilige Sicherheitstechnologie funktioniert, sowie eine Info-Box, die umstrittene Aspekte der Technologie darlegt. Der fünfte Abschnitt beschreibt jeweils kurz einige Alternativen zu Sicherheitstechnologien.

Wenn Sie nicht das ganze Dokument lesen wollen, dann finden Sie eine Zusammenfassung der wichtigsten Punkte auf der nächsten Seite.

2 Zusammenfassung

Das Ziel von SurPRISE ist es, die unterschiedlichen Ansichten europäischer BürgerInnen zu neuen Sicherheitstechnologien herauszufinden und zu verstehen. Da Europäische Regierungen immer besorgter über Terrorismus, organisierte Kriminalität und Cyberkriminalität wurden, haben diese verstärkt in die Entwicklung neuer Sicherheitstechnologien investiert. Viele dieser Technologien analysieren Informationen aus dem alltäglichen Leben, von uns allen. Zum Beispiel werden durch die Nutzung von Handys, dem Internet und mittels „intelligenter“ Technologien wie digitaler Videoüberwachung Informationen gewonnen, um Kriminelle oder Terroristen zu identifizieren, manchmal, bevor eine Tat überhaupt begangen wurde. Da diese Technologien persönliche Informationen verwenden, nennen wir sie „Überwachungs-basierte Sicherheitstechnologien“ (im Folgenden häufig abgekürzt mit „ÜBS“).

Eine überwachungs-basierte Sicherheitstechnologie ist...

... eine Technologie, die gesammelte Informationen aus verschiedenen Kontexten über die allgemeine Bevölkerung und ihre Aktivitäten verwendet um einem Sicherheitsproblem entgegenzuwirken.

Während der SurPRISE BürgerInnen-Foren werden wir diese drei Technologien genauer untersuchen:

- > **Smart CCTV:** Videoüberwachungssysteme, die über die bloße Überwachung des öffentlichen Raums hinausgehen. Smart CCTV verfügt über digitale Kameras, die an Systeme gekoppelt sind, die Personen identifizieren, ihr Verhalten analysieren und Objekte erfassen können.
- > **Cyber-Überwachung mit Deep Packet Inspection:** Mit Hardware-Geräten und spezieller Software können die Inhalte von Nachrichten (z.B. Texte und Bilder) die über das Internet übertragen werden, gescannt, analysiert und sogar verändert werden.
- > **Handyortung:** Durch die Analyse von Standortdaten eines Mobiltelefons können Informationen über Aufenthaltsort und Bewegungen des Handy-Nutzers über einen gewissen Zeitraum gesammelt werden. Der Standort eines Handys kann durch die

Daten der Sendemasten, Drahtlosverbindungen oder per satellitenbasiertem Global Positioning System (GPS) ermittelt werden.

Jede Technologie kann die Sicherheit durch Identifizierung von Verdächtigen und Kriminellen oder illegalen Aktivitäten verbessern. Manche glauben, dass diese Technologien das Leben einfacher gestalten können. Allerdings birgt jede Sicherheitstechnologie auch eine Reihe von Nachteilen in sich. Etwa funktioniert Smart CCTV nur unter bestimmten Bedingungen und kann eine Menge von „Fehlalarmen“ produzieren. Deep Packet Inspection bedroht die Privatsphäre der Online-Kommunikation enorm. Handyortung ist schwer kontrollierbar, weil viele Apps Standortdaten ohne Wissen der Handybenutzer automatisch übertragen. Die mangelnde Kontrolle über die Erhebung und Verwendung von Informationen ist bei allen Technologien, die wir untersuchen, ein kritischer Aspekt.

Abgesehen von den möglichen Sicherheitsgewinnen durch diese Technologien fühlen sich manche BürgerInnen unwohl, wenn ihre Daten für Sicherheitszwecke verarbeitet werden. Wenn sich die Sicherheit für alle dadurch erhöht, ist dies möglicherweise in Ordnung. Andererseits, wenn grundlegende Menschenrechte verletzt werden, kann dies wohl niemals in Ordnung sein. Die Meinungen der Menschen können zudem sehr unterschiedlich sein und von einigen weiteren Aspekten abhängen, zum Beispiel:

- > Sind diese Technologien eigentlich wirksam?
- > Wie weit dringen diese in die Privatsphäre ein?
- > Sind die Institutionen, die sie einsetzen vertrauenswürdig?
- > Gibt es genügend wirksame gesetzliche Regelungen?
- > Wer kontrolliert die Überwacher?
- > Was sind die Alternativen, und sind sie sinnvoll?

Dies sind einige der Fragen, die wir beim BürgerInnen-Forum diskutieren werden.

Wenn Sie mehr zu dieser Thematik erfahren wollen, lesen Sie bitte weiter.

3 Ein gewöhnlicher Tag...

Etwas südlich von Budapest ist Aisha auf der Europäischen Route E-75 auf dem Weg zum Flughafen. Sie erinnert sich zurück an das erste Mal, als sie diesen Weg benutzte. Da musste man die Mautgebühr noch sofort zahlen: Heute hingegen wird die Maut automatisch vom Konto abgebucht. Das Nummernschild wird durch die automatische Kennzeichenerfassung (Engl.: ANPR – Automated Numberplate Recognition) von Kameras erfasst und das Maut-System erledigt den Rest. Früher bemerkte Aisha die Kameras auf der Straße nicht. Heute fallen sie ihr auf und sie fragt sich, wie diese Informationen zu ihrer Bank gelangen.

Aisha parkt ihr Auto und fährt mit dem Shuttle-Bus zum Terminal. Dort checkt sie am Check-in Automaten gleich ein. Sie legt ihren Pass auf die Maschine und diese ordnet ihren Namen der entsprechenden Buchung zu. Beim Erhalt ihrer Bordkarte wird Aisha klar, dass auch hier Informationen über sie irgendwo gespeichert werden.

Nach der Sicherheitskontrolle setzt sich Aisha in ein Café und stellt ihr Handgepäck ab. Sie bestellt einen Kaffee, aber stockt kurz als sie an der Kassa ihre Geldkarte zu Bezahlung reicht. „Sehr praktisch, so ein Plastikding,“ denkt sie, „aber wer zeichnet diese Transaktion auf und warum?“

Während Aisha darauf wartet, dass ihr Kaffee etwas auskühlt, nimmt sie ihr Smartphone, um zu sehen, ob neue Nachrichten eingelangt sind. Als sie das Handy aktiviert, ändert sich am Startbildschirm sofort ihr Standort von ‚Kecskemét‘, wo Aisha wohnt, zu ‚Ferihegy‘. „Wie kann es das wissen? Es muss eine wirklich einleuchtende Erklärung dafür geben, aber ich kann es mir nicht erklären“, grübelt sie.

Aisha hat gerade einmal Zeit, eine E-Mail an einen Arbeitskollegen zu senden, bevor sie ins Flugzeug einsteigt. Als sie ihr Telefon auf ‚Flugmodus‘ stellt, fragt sie sich, was mit der E-Mail auf ihrem Weg durch das Internet passieren wird.

Aishas Reise ist nicht ungewöhnlich, sondern zeigt durchaus vertraute Ereignisse im Leben eines jeden Reisenden. Die Technologien bieten Vorteile für Aisha, indem sie die Reise bequemer und einfacher machen. Aber sie werfen für sie auch einige Fragen auf: „Wer nutzt meine persönlichen Daten und was bedeutet es für mich, dass diese jetzt ‚im System‘ sind?“

Viele der Technologien, mit denen Aisha konfrontiert ist, betreffen auch die Welt außerhalb des Flughafens. Viele Menschen können sich ein Leben ohne Smartphones, Geldkarten oder dem Internet nicht mehr vorstellen! Tatsächlich erzeugen wir in unserem Alltag unzählige elektronische Spuren, derer sich Aisha langsam bewusst wird. Vielleicht stellen Sie sich ähnliche Fragen wie Aisha. Diese Spuren können verraten, wann wir uns wo befinden, und manchmal auch was wir tun. Zum Beispiel sagen unsere Bankgeschäfte (vor allem mit Geld- und Kredit- oder Kundenkarten) etwas über unsere Einkaufsgewohnheiten aus, aber auch mit wem wir verkehren. Diese Informationen werden in Datenbanken gespeichert und wir können sie in unseren Kontoauszügen sehen.

Reisebuchungsinformationen geben Einblick, ob wir aus gefährlichen Regionen der Welt ein- oder in diese ausreisen. Handydaten zeigen, wo wir uns gerade befinden, wie häufig und mit wem wir kommunizieren. Diese Informationen werden von Telekommunikations- und Internetanbietern in deren Datenbanken gespeichert. Europäische Gesetze sehen vor, dass diese Daten zwischen sechs Monaten und zwei Jahren aufbewahrt werden müssen. So ist es möglich, Menschen zu verschiedenen Zeitpunkten ihres Lebens zu verfolgen und aufzuspüren. Das ist es vielleicht, was Aisha bedenklich stimmt. Aber sie ist auch hin- und hergerissen wegen der Vorteile, die diese Technologien versprechen.

Technologien wie die erwähnten und die Informationen, die sie sammeln, können auch von anderen genutzt werden. Nach aufsehenerregenden Terroranschlägen in Europa und anderswo haben Regierungen in neue Sicherheitstechnologien investiert, die diese Art von Informationen nutzen. Zusätzlich wurden bestehende Gesetze geändert und neue eingeführt, um Zugang zu diesen Informationen zur Gefahrenabwehr zu ermöglichen. Obwohl es viele „offizielle“ Informationsquellen für

Geheimdienste gibt, haben Regierungen weitere Maßnahmen ergriffen, um die Aktivitäten potenzieller Krimineller und Terroristen aufzudecken. Wie die Mehrheit der BürgerInnen besitzen auch Kriminelle und Terroristen Bankkonten, nationale Ausweisdokumente, nutzen das Internet und haben Handys. Sie benützen Verkehrsmittel, gehen auf öffentliche Plätze und konsumieren Waren und Dienstleistungen. Vielleicht könnte das Wissen über diese Aktivitäten der Schlüssel zur frühen Erkennung von Kriminellen und Terroristen sein. Viele Regierungen glauben, dass es durch den Einsatz neuer Sicherheitstechnologien nicht nur möglich sein wird, Übeltäter zu verhaften, sondern auch, sie frühzeitig zu erkennen, bevor sie Schaden anrichten. Technologien, welche die Verwendung dieser Informationen auf diese Weise ermöglichen, werden im Projekt SurPRISE als Überwachungs-basierte Sicherheitstechnologien (ÜBS) bezeichnet.

Eine überwachungs-basierte Sicherheitstechnologie ist...

... eine Technologie, die gesammelte Informationen aus verschiedenen Kontexten über die allgemeine Bevölkerung und ihre Aktivitäten verwendet um einem Sicherheitsproblem entgegenzuwirken.

Wenn Aisha bewusst wäre, dass ihre Informationen auf diese Weise zu Sicherheitszwecken verwendet werden könnten, wäre sie dann immer noch im Zwiespalt? Wenn es mehr Sicherheit für alle bedeuten würde, vielleicht wäre das dann etwas, was sie akzeptieren könnte. Der Einsatz dieser Technologien wirft allerdings Fragen über Menschenrechte, Privatsphäre, Regulierung und Vertrauen auf. Schließlich sammeln und verarbeiten diese Technologien Informationen über Personen auch ohne deren Wissen. Auch Daten über unschuldige Personen werden zwangsläufig erfasst und analysiert, bei manchen Technologien geschieht dies sogar absichtlich. Das kann zu tiefen Eingriffen in die Privatsphäre führen, die in Europa als grundlegendes Menschenrecht geschützt ist. Auch Unschuldige können fälschlicherweise als Bedrohung eingestuft werden, mit ernsthaften Konsequenzen für das Leben dieser Personen.

Das wirft eine Reihe von Fragen auf:

- > Sind die Institutionen, die diese Daten verwenden vertrauenswürdig?
- > Wie klar ist der Umgang mit den Daten durch diese Institutionen gesetzlich geregelt?
- > Sind die eingesetzten Technologien gesetzeskonform?
- > Sind die Institutionen transparent und rechenschaftspflichtig für etwaige Verstöße gegen die Privatsphäre, die im Namen der Sicherheit begangen werden?
- > Erhöhen diese Technologien wirklich die Sicherheit?

Dies sind einige der Fragen, die wir bei dem BürgerInnen-Forum untersuchen werden.

In den nächsten Absätzen werden einige der wichtigsten Begriffe und Definitionen erläutert, bevor die Technologien beschrieben werden, die wir in den Foren behandeln werden.

3.1 Überwachung, Privatsphäre und Sicherheit

3.1.1 Überwachung

Wenn wir an Überwachung denken, tauchen wahrscheinlich gleich einige Bilder vor Ihnen auf: Sie denken vielleicht an „Big Brother“, beides – sowohl die Reality Show als auch den „Großen Bruder“ als Sinnbild des Diktators in George Orwells Roman 1984. Demzufolge verbinden Sie mit Überwachung möglicherweise das beklemmende Gefühl, von einer mächtigen, unbekannten Organisation oder Person beobachtet werden.

Wenn wir in SurPRISE von „Überwachung“ sprechen, meinen wir damit das Beobachten von Personen, um ihr Verhalten zu regeln oder zu steuern. Dies kann verschiedene Gründe haben. Überwachung kann für Sicherheitszwecke eingesetzt werden. Etwa könnte die Polizei Videoüberwachung einsetzen, um Übeltäter im öffentlichen Raum aufzuspüren. Überwachung kann aber auch aus kommerziellen Zwecken erfolgen. Zum Beispiel könnte ein Supermarkt mittels Kundenkarten die Kaufgewohnheiten verschiedener Kundengruppen herausfinden, um den Kunden dann jeweils unterschiedliche Sonderangebote anzuzeigen. Mit Überwachung kann versucht

werden, Kriminalität zu verhindern und Kriminelle zu fangen, aber auch, Produkte und Dienstleistungen zu bewerben.

Wenn Überwachung zu einem normalen Bestandteil der Gesellschaft geworden ist, dann fragen Sie sich vielleicht, was daran falsch sein soll.

Berichte in den Nachrichten bezüglich „Überwachungsgesellschaft“ scheinen immer einen bitteren Beigeschmack zu haben. Der springende Punkt ist, dass die Kontrolle über eine Überwachungstechnologie große Macht verleiht. Es ist wichtig, dass alle jene, die in solchen Positionen sind, wie etwa Strafverfolgungsbehörden, Datenhändler oder Unternehmen, diese Macht verantwortungsbewusst, fair und unter Wahrung von Bürgerrechten und Gesetzen ausüben.

Ob Sie denken, nichts zu verbergen oder nichts zu befürchten zu haben, hängt tatsächlich stark davon ab, wer überwacht, warum überwacht wird, und wie Ihre Handlungen von den ÜberwacherInnen wahrgenommen werden. Wenn Sie keine Kontrolle oder Mitsprache in diesem Prozess haben und sich die Regeln und Gesetze plötzlich gegen Sie richten – etwa aufgrund Ihrer ethnischen Herkunft, Religion, sexuellen Orientierung, ihres Geschlechts oder ihrer politischen Ansichten – was würden Sie tun? Das ist ein Grund, warum Überwachung negative Folgen auf weitere Menschenrechte, wie Meinungsfreiheit, haben kann. Solche Folgen können zudem zur Erosion des sozialen Vertrauens im Allgemeinen führen, da Menschen Angst davor bekommen, sie selbst zu sein, und glauben, sich verstellen zu müssen. Sehr vieles steht auf dem Spiel, wenn verschiedene Überwachungsdaten zu Sicherheitszwecken verwendet werden.

3.1.2 Privatsphäre und Datenschutz: Wichtige Aspekte?

Eine der zentralen Fragen betrifft den Schutz der Privatsphäre, und wie die von neuen Sicherheitstechnologien erzeugten und verwendeten Daten geschützt werden können. Privatsphäre kann für unterschiedliche Menschen unterschiedliche Dinge bedeuten. Unabhängig davon ist der Schutz der Privatsphäre ein wesentlicher Bereich des täglichen Lebens. Es gibt vermutlich eine Reihe von Dingen, die Sie zumeist für sich behalten wollen:

- > Informationen über Ihre intimen Beziehungen, wo Sie sich aufhalten, worüber Sie mit anderen sprechen oder kommunizieren (egal ob persönlich, per Post oder E-Mail), Ihre persönlichen Eigenheiten, oder Bilder von Ihnen
- > Ihr Körper: Wie viel davon Sie enthüllen, ob Sie ihn vor ungewünschter Berührung oder Leibesvisitation bewahren können, sowie die Kontrolle über die Verwendung Ihrer Körpermerkmale, wie Ihre DNS oder Ihre Fingerabdrücke.

Denken Sie darüber nach: Wären Sie einverstanden, wenn eine Lebensversicherungsgesellschaft uneingeschränkten Zugang zu Ihren Gesundheitsdaten hätte? Oder wenn die Polizei all Ihre Telefonate abhören könnte? Haben Sie zuhause Vorhänge? Egal, ob Sie alle, oder nur eine dieser Fragen mit „ja“ beantworten – Ihre Privatsphäre ist Ihnen nicht gleichgültig. Sie sind damit nicht alleine. Studien belegen, dass Jugendliche bei der Nutzung sozialer Netzwerke aufgrund von Datenschutzbedenken zum Teil nur ausgewählte Informationen preisgeben. Die Menschen wollen zwar Informationen teilen, allerdings nicht beliebig, sondern innerhalb definierter Bereiche. Für das Individuum gilt alles, was über diese Bereiche hinausreicht, als Bereich des Lebens, der frei von äußerlichen Eingriffen bleiben soll: Ihr Privatleben.

In SurPRISE definieren wir Privatsphäre als die Fähigkeit eines Individuums, selbstständig, unbeobachtet, selbstbestimmt und mit Kontrolle über die eigenen Informationen zu handeln.

Das Recht auf Privatsphäre und das Recht auf den Schutz personenbezogener Daten sind wichtige Grundrechte in der Europäischen Union. Jede/r benötigt diese Rechte, um in einer demokratischen Gesellschaft frei handeln, sich treffen und diskutieren zu können. Die Menschen können ihre demokratischen Freiheiten nicht ausüben, wenn alles über ihre Gedanken, Absichten und Handlungen offengelegt wird. Neue Europäische Datenschutzgesetze sollen dafür sorgen, dass Datenschutz ein integraler Bestandteil neuer Technologien wird, damit diese bereits von vornherein weniger bedrohlich für die Privatsphäre sind. Unternehmen sollen ermutigt werden, die Privatsphäre Schritt für Schritt im Entwicklungsprozess zu berücksichtigen. Dieser neue Ansatz nennt sich „Privacy by Design“.

- > Was Sie tun, denken und fühlen

3.1.3 Sicherheit

In SurPRISE definieren wir Sicherheit als Zustand des Beschütztseins vor Gefahren; einem Gefühl der Gefahrlosigkeit frei von Bedrohung.

Sicherheit bezieht sich nicht nur auf physische Dinge wie Gebäude, Informationssysteme, nationale Grenzen usw., sondern bezieht sich auch auf menschliche Gefühle von Gefahrlosigkeit und Geborgenheit. In einer idealen Welt würden effektive Sicherheitsmaßnahmen zu mehr Sicherheit führen. Doch das ist nicht immer der Fall.

Es erscheint befremdlich, dass neue Sicherheitstechnologien die Privatsphäre bedrohen können, und wir uns daher sogar deutlich unsicherer statt sicherer fühlen. Doch das muss nicht für jeden gleich sein. Wie die Privatsphäre kann auch Sicherheit für verschiedene Menschen eine sehr unterschiedliche Bedeutung haben. Jede/r von uns hat ihre/seine eigenen Vorstellungen darüber, was als Sicherheitsbedrohung wahrgenommen wird, und wie wir uns verhalten, um Dinge, die uns wichtig sind zu schützen.

Das gilt auch für jene, die für die Sicherheit verantwortlich sind. Sie müssen die wichtigsten Gefahren erkennen und damit umgehen. Jede Regierung verfügt nur über eingeschränkte wirtschaftliche, menschliche und technische Mittel zur Wahrung von Sicherheit und muss dementsprechend Entscheidungen treffen. Für die Europäische Union sind die wesentlichen Sicherheitsprioritäten:

- > Erhöhung der Cyber-Sicherheit für BürgerInnen und Unternehmen in der EU
- > Zerschlagung von internationalen kriminellen Netzwerken
- > Verhinderung von Terrorismus
- > Stärkung der Widerstandsfähigkeit Europas im Umgang mit allen Arten von Krisen oder Katastrophen.

Da Europa beschlossen hat, sich auf die Widerstandsfähigkeit im Umgang mit allen Arten von Krisen oder Katastrophen zu konzentrieren, reicht Sicherheit nun über die Bekämpfung von Verbrechen und Terrorismus hinaus. Europa befasst sich auch mit Gefahren für die Umwelt, natürlichen Ressourcen, Infrastruktur, wirtschaftlichen Aktivitäten und Gesundheit. Für politische Entscheidungsträger umfasst Sicherheit mittlerweile nahezu alle Bereiche des öffentlichen Lebens. Dieses Verständnis

wurde in vielen Europäischen Ländern übernommen. Aber kann das Versprechen von Sicherheit in all diesen Bereichen jemals eingehalten werden? Die Sicherheitsindustrie ist ein gewichtiger Bereich geworden, der auch in Europa wächst, und sich mit dem erweiterten Sicherheitsverständnis befasst. Große Rüstungskonzerne wie Airbus, BEA Systems und Finmeccanica sowie eine Vielzahl kleinerer Unternehmen sind ein Teil davon. Jüngste Entwicklungen im Bereich überwachungsbasierter Sicherheitstechnologien umfassen vor allem:

- > Intelligente Videoüberwachung (Smart CCTV), die darauf abzielt, Straftäter aufzuspüren sowie verdächtiges Verhalten zu erkennen
- > Cyber-Überwachung, die versucht, Gefahren wie Viren, Hackerangriffe oder Identitätsdiebstähle zu bekämpfen
- > Biometrie, die u.a. eingesetzt wird, um unerwünschte Personen an der Einreise zu hindern sowie die Passierabfertigung für „vertrauenswürdige Reisende“ zu beschleunigen
- > Moderne Passagierinformationssysteme, um gefährliche Personen schon vor ihrer Reise aufzuspüren
- > Ortungstechnologien, um Schaden durch bewegliche Dinge zu minimieren, sowie Verdächtige zu lokalisieren.

4 Drei neue Sicherheitstechnologien

SurPRISE untersucht bei den BürgerInnen-Foren die folgenden Technologien:

- > **Smart CCTV
(Intelligente Videoüberwachung)**
- > **Cyber-Überwachung am Beispiel
Deep Packet Inspection**
- > **(Smart) Phone location tracking
(Ortung von Mobiltelefonen)**

Diese Sicherheitstechnologien sind gerade im Entwicklungsstadium, und die gesellschaftlichen Rahmenbedingungen sind größtenteils noch nicht festgelegt.

Die folgenden Abschnitte erläutern, wie diese Technologien funktionieren, warum sie

entwickelt werden, von wem und wozu sie verwendet werden. Auch die möglichen Sicherheitsverbesserungen sowie Aspekte der Privatsphäre und verwandte Themen werden behandelt.

Es ist wesentlich für dieses Projekt und die Europäische Union, besser zu verstehen, was Menschen über Sicherheitstechnologien denken, und wie akzeptabel sie diese finden. Deshalb ist Ihre Meinung so wichtig. Sie haben möglicherweise bereits eine ausgeprägte Meinung, pro oder contra, zu bestimmten Technologien. Im Lauf des SurPRISE-Forums werden Sie viele Gelegenheiten haben, Ihre Meinung zu äußern. Im Speziellen geht es uns vor allem um folgende Fragen:

Was macht eine neue Sicherheitstechnologie mehr oder weniger akzeptabel für Sie?

Könnte es sein, dass Sie:

- > Mehr über die Technologie wissen wollen, und wie sie funktioniert?
- > Mehr über die verschiedenen Institutionen wissen wollen, die diese Technologie einsetzen, sowie über die Informationen, die damit gewonnen werden?
- > Effektive gesetzliche Rahmenbedingungen und Kontrollmechanismen haben wollen?
- > Über die verschiedenen Bedrohungen, die diese Technologien bekämpfen sollen, besser informiert werden wollen?

Oder hängt es davon ab, für wie bedrohlich Sie die Technologie selbst halten.

Zum Beispiel:

- > Verursacht sie irgendwelche Unannehmlichkeiten?
- > Verletzt sie die Grundrechte?
- > Verrät sie Informationen an Dritte ohne Ihr Wissen oder Einverständnis, oder hat sie andere Auswirkungen auf Ihre Privatsphäre?

Vielleicht hängt es davon ab, wie effektiv die Technologie ist:

- > Macht sie das Leben angenehmer?
- > Fühlen Sie sich dadurch sicherer?
- > Sind Sie der Meinung, dass sie treffsicher Verdächtige identifiziert?

Oder vielleicht kümmern Sie Sicherheitstechnologien nur dann, wenn Sie unmittelbar in Ihrer Nähe eingesetzt werden. Das könnte am Flughafen, auf der Straße sein, oder wenn Sie ein Mobiltelefon benutzen, oder im Internet surfen. Die restliche Zeit kümmert Sie das nicht. Vielleicht haben Sie derzeit kein Problem mit Sicherheitstechnologien, aber vielleicht haben Sie Bedenken über deren Verwendung in der Zukunft.

5 Intelligente Videoüberwachung – Smart CCTV¹

In Abschnitt 3 dieser Broschüre ist beschrieben, wie sich Aisha auf ihrem Weg zum Flughafen fragt, wie die Kameras zur Straßenmarterfassung funktionieren. Kameras, die Kennzeichen oder andere Merkmale automatisch erfassen können, sind ein Beispiel für eine neue Sicherheitstechnologie – das sogenannte „Smart CCTV“ oder „intelligente Videoüberwachung“.

Die meisten EuropäerInnen sind vertraut mit Videoüberwachungssystemen. Herkömmliche Videoüberwachungssysteme sind mit Kameras ausgestattet, die z.B. an öffentlichen Plätzen oder in Geschäften montiert sind. Die Kameras sind mit einem Kontrollraum verbunden. Im Kontrollraum sind zahlreiche Monitore, die dem Überwachungspersonal zeigen, was die Kameras erfassen. Die Bilder werden aufgezeichnet, gespeichert und nach einer bestimmten Zeit gelöscht. Das System ist „geschlossen“, weil die Bilder nicht außerhalb des Kontrollraums übertragen werden. Wenn das Überwachungspersonal etwas Verdächtiges beobachtet, können Sicherheitskräfte gerufen werden, um einzugreifen.

5.1 Warum Smart CCTV entwickelt wurde

Videoüberwachung wurde ursprünglich entwickelt, um Raketenstarts im Zweiten Weltkrieg und gefährliche Betriebsprozesse aus sicherer Distanz zu beobachten. Erstmals wurde sie in den 50er Jahren in den USA als Sicherheitstechnologie verkauft, in den 1960er Jahren schließlich von der Polizei in den USA und Großbritannien eingesetzt. In Europa nahm der Einsatz von Videoüberwachung in den 1990er Jahren kontinuierlich zu, vor allem in England, gefolgt von Frankreich und den Niederlanden. Videoüberwachung ist häufig in den Medien vertreten. Etwa wurde 2013 nach dem Anschlag beim Boston-Marathon über die Rolle von Überwachungskameras zur Identifizierung der Attentäter berichtet.

Smart CCTV wurde entwickelt, um ein Grundproblem von Videoüberwachung zu

¹ CCTV steht für „Closed Circuit Television“ und ist der englische Begriff für Videoüberwachung.



bewältigen: Den Umstand, dass Kameras zu viele Bilder liefern, und zu wenig Personen verfügbar sind, um diese auszuwerten. Im Gegensatz zu herkömmlicher Videoüberwachung verwendet Smart CCTV miteinander vernetzte digitale Kameras, die an Analyse-systeme gekoppelt sind. Eine entsprechende Software analysiert, was die Kamera beobachtet. Wenn etwas Ungewöhnliches geschieht, wird ein Alarm ausgelöst, um das Überwachungspersonal darauf hinzuweisen. Das alarmauslösende Ereignis wird gespeichert und ist jederzeit abrufbar.

Smart CCTV Software kann eine Reihe von Dingen. Insbesondere wird sie verwendet zur:

- > Identifikation eines Objektes in einem Bild; etwa ein Fahrzeug, durch Auslesen des Kennzeichens und Abgleich dieser Information mit einer Datenbank.
- > Identifikation des Gesichts einer Person, wenn das Gesicht auf einem klaren, einfarbigen Hintergrund erscheint. Abgleich des Gesichts mit einer Datenbank mit amtsbekannten Personen.
- > Detektion unbeaufsichtigter Gegenstände wie Taschen an öffentlichen Plätzen.

Obwohl Smart CCTV die folgenden Dinge derzeit nicht verlässlich leisten kann, wird Software entwickelt um:

- > Personen anhand ihrer Kleidung in größeren Menschenmengen zu identifizieren
- > Verdächtiges Verhalten zu erkennen, oder Verhalten, das ungewöhnlich wirkt, wie etwa längeres Herumstehen in einem Durchgangsbereich. Beobachtetes Verhalten wird mit bekannten Verhaltensmustern verglichen, die in Datenbanken gespeichert sind.



Nicht alle Smart CCTV Systeme sind gleich. Wie „intelligent“ ein System ist, hängt davon ab, wie gut die Software die Bilder analysiert, und was mit den Bildern geschieht. Systeme werden für verschiedene Zwecke eingesetzt. Ein Smart CCTV System muss also nicht alle der vorhin genannten Dinge können. Für Betreiber solcher Systeme sind vielleicht nicht alle diese Dinge notwendig.

Wie funktioniert Smart CCTV?

Mit Hilfe intelligenter Algorithmen lernt ein Smart CCTV System, bestimmte Verhaltensmuster zu erkennen. Diese werden als sogenannte „Trigger Events“, also auslösende Ereignisse bezeichnet. Zum Beispiel eine Person, die eine Waffe hält oder bewegungslos in einer bewegten Menschenmenge steht. Ein Algorithmus ist eine Kette von Rechenvorgängen, die Daten des digitalen Kamerabildes auswertet. Ein intelligenter Algorithmus ist lernfähig und lernt, indem er immer mehr Daten analysiert.

Intelligente Algorithmen in Smart CCTV Systemen werden entwickelt, um nachzuvollziehen, wie menschliches Verhalten funktioniert. Die Software zerlegt ein Bild in winzige Einzelteile, sogenannte Pixel (Bildpunkte). Sie kennen den Begriff vermutlich, wenn Sie eine Digitalkamera haben. Eine Kamera mit 8 Megapixel bedeutet, dass jedes aufgenommene Bild aus 8 Millionen Pixeln besteht.

Der Algorithmus ist in der Lage, den Bewegungsgrad jedes Pixels im Bild zu berechnen. Das ermöglicht der Software, die aktiven Bereiche in jeder Szene zu erkennen. Anhand dessen lernt sie, die Bewegungsmuster in einer Aufnahme zu erkennen. Das System kann dann Ereignisse anhand der bereits bekannten Muster erkennen und einstufen. Zum Beispiel kann die Software zwischen passiven Zuschauern und herumhüpfenden Fans bei einem Fußballspiel unterscheiden.

5.2 Wie Smart CCTV verwendet wird

Smart CCTV Systeme sind kommerzielle Produkte, die von Sicherheits- und Verteidigungsunternehmen verkauft werden. Viele Systeme sind bereits verfügbar. Derzeit sind Verkehrsbetriebe (die etwa öffentliche Straßen, Flughäfen oder Bahnhöfe verwalten), Verwaltungsbehörden und die Polizei die institutionellen Hauptanwender von Smart CCTV.

In Budapest begann die Polizei Ende 2012, Smart CCTV zu nutzen, um Busstrecken zu überwachen. Die Polizei darf die Bilder rechtmäßig verwenden, sofern keine Passagiere gefilmt werden und die Öffentlichkeit vollständig informiert wird. Am Flughafen in Zürich sind seit 2003 Gesichtserkennungskameras im Einsatz. Damals wurde diese Technologie zum allerersten Mal für Grenzkontrollen eingesetzt. Heute ist dieses System permanent in Betrieb.

Die Europäische Union hat 16 verschiedene Projekte gefördert, die die Algorithmen und Funktionen von Smart CCTV Systemen erforschen. Komplexere Aufgaben, wie das Erkennen verdächtigen Verhaltens oder von Gesichtern in Menschenmengen, werden noch entwickelt und verbessert. Diese Anwendungen sind noch nicht weit verbreitet und neue Systeme werden laufend getestet, z.B. in Rom, London, Paris, Brüssel, Mailand und Prag.

Wohl am weitesten verbreitet ist der Einsatz von Smart CCTV bei der automatischen Kennzeichenerfassung. Anhand des digitalen Bildes eines KFZ-Kennzeichens können Informationen mit verschiedenen Datenbanken abgeglichen werden, z.B. von KFZ-Registrierungsstellen, Versicherungen und der Polizei. Der/Die KFZ-BesitzerIn und das registrierte



Fahrzeug können einfach ermittelt werden, und das Kennzeichenerfassungssystem kann das betreffende Fahrzeug lokalisieren. Das System kann verwendet werden, um Fahrzeuge zu identifizieren, die gestohlen oder nicht registriert sind, ohne Mautplakette oder Versicherung unterwegs sind, oder zu schnell fahren.

Eine Frage ist, ob diese unterschiedlichen Arten von Vergehen dasselbe Ausmaß von Überwachung rechtfertigen. Soll Smart CCTV wirklich für alle Arten von Vergehen eingesetzt werden oder nur bei schwereren Straftaten? Es gibt unterschiedliche Ansichten darüber in Europa. In Deutschland etwa schränkte das Bundesverfassungsgericht 2008 den Einsatz von automatischer Kennzeichenerfassung bei der Polizeiarbeit aufgrund von Verletzungen der Privatsphäre ein. Das Gericht entschied, dass die Polizei die erfassten Daten nur für den unverzüglichen Abgleich mit Fahndungsdaten nutzen darf und ansonsten Nicht-Treffer ohne weitere Auswertung sofort zu löschen sind. Automatische Kennzeichenerfassung wurde auch genutzt, um Straßenmaut zu erheben aber nach vermehrter Kritik wurden andere, weniger überwachungsorientierte Mittel dafür gefunden. In England ist die Lage etwas anders; hier hat auch die Polizei laufend Zugang zu solchen Mautsystemen.

Umstrittener Einsatz von Smart CCTV: Automatische Kennzeichenerfassung in Birmingham

Im Jahr 2011 musste die Polizei in Birmingham, England, Kameras zur automatischen Kennzeichenerfassung in drei Bereichen der Stadt mit hohen muslimischen Bevölkerungsanteilen wieder entfernen. Das Anti-Terrorismus Programm „Projekt Champion“ subventionierte den Kameraeinsatz. Die offizielle Begründung für die Öffentlichkeit lautete dagegen nur allgemein „aus Sicherheitsgründen“. Mitglieder der Gemeinde sowie des Regionalparlaments äußerten schwere Bedenken und es kam zu Spannungen zwischen verschiedenen Nachbarschaften. 200 Kameras wurden installiert, aber nie in Betrieb genommen. 64 Kameras waren versteckt und ohne öffentliche Genehmigung eingesetzt. Nach Protesten wurden die Kameras zum Teil zerstört oder von anderen Polizeibehörden verwendet.

Das Scheitern des Projekts kostete umgerechnet € 351.414,-.

5.3 Verbesserungen im Bezug auf die Sicherheit

Smart CCTV kann die Sicherheit in den folgenden Bereichen verbessern:

1. Sicherheitsprobleme sind leichter zu erkennen, wenn sie auftauchen:
 - > Das System erkennt alles Ungewöhnliche und alarmiert das Wachpersonal.
 - > Der Alarm erleichtert es dem Wachpersonal, schnellere, effizientere Entscheidungen zur Bewältigung des Sicherheitsproblems zu treffen.
 - > Die Algorithmen im System sind in der Lage, rasch enorme Informationsmengen zu verarbeiten. Dadurch können sie Details erfassen, die manchmal vom Personal übersehen werden könnten.
2. Angst vor Verbrechen und Übergriffen kann reduziert werden:
 - > Wenn die Sicherheitstechnologie effektiv arbeitet, sind die Menschen beruhigt, weil sie davon ausgehen, dass ungewöhnliche Ereignisse um sie herum von Smart CCTV schnell erkannt werden.
 - > Die digitalen Kameras bei Smart CCTV sind leistungsfähiger als herkömmliche Kameras. Dadurch werden zum Teil auch weniger Kameras zur Überwachung benötigt. Als Resultat wirken diese weniger aufdringlich.
 - > Datenschutz kann verbessert werden, indem sensible Bereiche wie etwa Einblicke in private Häuser geschwärzt werden, sodass das Bedienungspersonal diese Bereiche nicht sieht.

5.4 Kritische Aspekte

Einige Schattenseiten von Smart CCTV müssen allerdings beachtet werden:

1. Die derzeit eingesetzten Smart CCTV Algorithmen weisen eine Reihe von Problemen und Schwachstellen auf. Diese Schwächen können zu Fehlalarmen führen, wodurch falsche Sicherheitsvorfälle gemeldet werden. Das kann dazu führen, dass Unschuldige mit Verdächtigen verwechselt werden. Derzeitige Schwächen sind:
 - > Nur bestimmte Objekte, wie etwa KFZ-Kennzeichen oder unbeaufsichtigte Taschen können verlässlich identifiziert werden.
 - > Die Systeme sind bisher kaum in der Lage zu erkennen, was in einer Menschenmenge geschieht.
 - > Verbrechen im Verborgenen, wie Taschen- oder Ladendiebstahl sind schwer zu erkennen.
 - > Die Algorithmen sind anfällig für Verzerrungen, weil sie von Menschen programmiert werden, die selbst und eventuell willkürlich festlegen, welches Verhalten als „abnormal“ gelten soll. Es besteht die Gefahr, dass diese Systeme absichtlich oder unabsichtlich, für bestimmte Personen oder Gruppen diskriminierend sind.
 - > Da die Systeme die Kleidung zur Erkennung von Verdächtigen heranziehen, könnten künftig mögliche Kriminelle die davon wissen, einfach durch Ändern ihrer Kleidung untertauchen.
 - > Die hohe Anzahl von Fehlalarmen könnte dazu führen, dass das Vertrauen in das System sinkt, und letztlich auch echte Alarme ignoriert werden.

2. Intelligente Überwachungskameras sind viel leistungsfähiger und auch kleiner:
 - > Sie können sehr viele Informationen erfassen und greifen so auch viel weiter in die Privatsphäre ein. Auf diese Weise ist es wahrscheinlicher, dass auch die Handlungen von Unschuldigen erfasst und analysiert werden.
 - > Die Kameras sind weniger einfach zu erkennen. Dadurch wird es für Menschen schwieriger zu bemerken, dass sie überwacht werden. Menschen können sich der Überwachung dadurch immer weniger entziehen.
 - > Meinungsfreiheit und Menschenwürde jeder/s Einzelnen können betroffen sein, wenn die Öffentlichkeit weiß, dass ihr Verhalten auf diese Weise überwacht wird.
3. Nach wie vor sind Menschen notwendig, um die Systeme zu bedienen. Das bedeutet:
 - > Ein Mensch wird benötigt, um die Bilder zu interpretieren und zu prüfen, ob ein Alarm gerechtfertigt ist. Das System kann zwar ungewöhnliches Verhalten erkennen, jedoch nicht, wie es dazu kommt.
 - > Institutionen müssen sehr gründlich reguliert und kontrolliert werden, um die möglichen weitreichenden Suchfunktionen einzugrenzen und vor Datenmissbrauch zu schützen.



Transparenz darüber, warum Smart CCTV eingesetzt wird, ist unerlässlich. Die Menschen sollten berechtigt sein, den Betreiber eines Systems zu kontaktieren, um Auskunft über den Zweck des Systems zu erhalten. Die Menschen müssen das Gefühl haben, dass die Kamera für einen sinnvollen Zweck eingesetzt wird, und sie müssen Klarheit über die Verwendung haben.

Chris Tomlinson, Sicherheitsplaner

6 Cyber-Überwachung durch Deep Packet Inspection

Als sie am Flughafen im Kaffeehaus saß, fragte sich Aisha, was mit ihrer E-Mail, die sie ihrem Kollegen geschickt hatte, auf deren Weg durch das Internet geschieht. Es könnte Gegenstand einer Form der Cyber-Überwachung geworden sein, der sogenannten „Deep Packet Inspection“, einer speziellen Technik der Netzwerküberwachung, die den Inhalt von Datenpaketen kontrolliert.

Internetdiensteanbieter, Netzbetreiber und Telekommunikationsfirmen waren seit jeher in der Lage, ihre Netzwerke zu überwachen. Zu wissen, wer mit wem kommuniziert, welche Webseiten besucht werden und welche Anwendungen genutzt werden, liefert Informationen für Kundenabrechnungen, Netzwerkmanagement und Marketing-Aktivitäten dieser Unternehmen. Allerdings befähigt eine Technik namens „Deep Packet Inspection (DPI)“ Unternehmen, Geheimdienste und Regierungen dazu, sogar den Inhalt von Nachrichten zu lesen, die übers Internet versendet werden. Um die Tragweite von DPI zu veranschaulichen, können Sie sich den Vorgang ähnlich vorstellen, wie ein Postamt, das alle Briefe öffnet, sie liest, manche davon verändert, löscht oder gar nicht zustellt. DPI ist in der Lage, jede Form der digitalen Kommunikation zu überwachen. Das reicht von der Information, die sie online lesen, den Webseiten die sie besuchen, den Videos die sie sich ansehen, ihre Suchbegriffe in Suchmaschinen, bis zu Daten darüber, mit wem sie worüber kommunizieren, egal ob per E-Mail, sozialen Netzwerken oder anderen Kommunikationsdiensten. DPI Anwendungen funktionieren durch die Erfassung und Beeinflussung der Art, wie Nachrichten in einem Netzwerk übertragen werden. Sie öffnen und analysieren Nachrichten sobald sie unterwegs sind und identifizieren jene, die mögliche Risiken in sich bergen. Sie müssen kein Verdächtiger sein, um von DPI betroffen zu sein – DPI fängt jede Nachricht, die durch das Netzwerk eines Internetproviders übertragen wird, ab und liest den Inhalt aus.



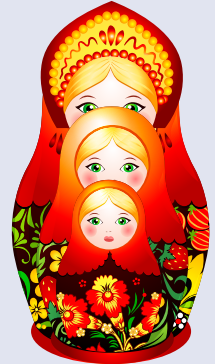
6.1 Wozu Deep Packet Inspection entwickelt wurde

DPI wurde ursprünglich entwickelt, um Viren und Schadsoftware zu erkennen, die Computernetzwerke gefährden. Heutzutage kann DPI durch die Analyse von Nachrichteninhalten auch dazu verwendet werden, gefährliche oder kriminelle Aktivitäten im Internet zu erkennen.

Wie Deep Packet Inspection funktioniert

Wenn Sie irgendeine Information über das Internet versenden oder empfangen, durchläuft diese Information zahlreiche sehr komplexe Prozesse entlang vieler verschiedener Computer.

Computer, die über das World Wide Web miteinander verbunden sind, zerlegen die Information in kleine Stücke, sogenannte „Datenpakete“. Dadurch kann Information einfach und schnell übertragen werden. Wenn die Pakete an ihrem Ziel ankommen, werden sie wieder zur gesamten Nachricht zusammengefügt. Jedes Paket hat eine Art Umschlag den sogenannten ‚Header‘: dieser beschreibt die Art des Pakets, von wem es ist und wohin es geht, ähnlich wie der Umschlag und die Adressaufschriften eines Briefes per Post. Die sog. ‚Payload‘ also die Nutzlast, bezeichnet den Inhalt eines Pakets, also im übertragenen Sinne den Inhalt des Briefes.



Jedes Paket hat mehrere Schichten, jede enthält unterschiedliche Informationen über die Nachricht: Die Schichten bauen aufeinander auf, ein wenig vergleichbar mit einer Russischen Puppe (Matroschka), die aus kleineren Puppen besteht. Internetprovider müssen einige der Pakete einer Nachricht untersuchen, damit sie übertragen werden kann. Meistens reicht es, wenn nur die Header (also der Umschlag) gelesen wird und nicht den Inhalt (das Innere des Umschlags), um eine Nachricht sicher ans Ziel zu bringen. Das wird ‚Shallow Packet Inspection‘ genannt. Deep Packet Inspection geht dagegen viel weiter und untersucht sämtliche Pakete und den Nachrichteninhalt.

Die Pakete werden mit Hilfe von Algorithmen analysiert, die nach bestimmten Datenarten suchen. Diese Algorithmen sind teilweise vergleichbar mit jenen, die im Abschnitt über Smart CCTV erläutert wurden, werden aber in anderer Weise verwendet.

Bei DPI suchen Algorithmen nach bestimmten Schlüsselwörtern, ähnlich wie bei einer Suche im Internet. Nach welchen Daten gesucht wird, hängt davon ab, von wem und wofür DPI eingesetzt wird. Die Schlüsselwörter könnten auf kriminelle oder verdächtige Aktivitäten verweisen, auf einen neuen Computervirus oder sogar darauf, ob ein bestimmtes Produkt gekauft wurde.

Deep Packet Inspection findet meist in sogenannten ‚Routern‘ statt. Ein Router ist ein Netzwerkgerät, das dafür sorgt, dass Nachrichten über die verschiedenen miteinander verbundenen Netzwerke des Internet weitergeleitet werden. Internetprovider verfügen über die gesamte technische Ausstattung, auf der DPI beruht. Diese Unternehmen können kontrollieren, wie das Internet lokal, regional, national oder international funktioniert. Es sind vor allem Netzwerkunternehmen, die die Technologie für DPI auf den Weg gebracht haben. Unternehmen setzen die Technologie für ihre eigenen Zwecke ein, können aber auch Profit daraus schlagen, wenn sie ihre Innovation an andere verkaufen. Zudem haben auch weitere Unternehmen, etwa im Verteidigungsbereich, DPI entwickelt und wollen es dementsprechend einsetzen. Es gibt mittlerweile einen Markt für DPI-Technologie.

6.2 Wie Deep Packet Inspection funktioniert

In Europa ist der Einsatz von DPI rechtlich beschränkt. Gemäß der geltenden Gesetze kann es verwendet werden, um Internetverkehr zu filtern, mit dem Ziel Viren oder Schadprogramme auszusondern. Internetunternehmen nutzen es vor allem zum Lastmanagement in ihren Netzwerken. Aber DPI ist auch in der Lage, den gesamten Inhalt von Online-Kommunikation zu analysieren. Wenn es auf diese Weise genutzt wird, kann es auch zur Erkennung bestimmter Verbrechen, wie etwa die Verbreitung von Kinderpornographie, eingesetzt werden. Doch das ist rechtlich höchst umstritten, da es kein Gesetz gibt, dass die Nutzung von DPI im Detail regelt. Das liegt daran, dass die Europäischen Gesetze, die u.a. Informationstechnologien regulieren, zu einer Zeit geschaffen wurden, als es noch kein DPI gab. Der Europäische Gerichtshof sowie der

Europäische Datenschutzbeauftragte stellten fest, dass diese Gesetze nur auf eingeschränktes ‚Filtern‘ von Online-Kommunikation Bezug nehmen. Neue Gesetze müssen entwickelt werden, welche die Verwendung von DPI detaillierter und angemessener regulieren.

Die Verwendung von DPI zur allgemeinen Überwachung von Kommunikation, sei es um Urheberrechtsverstöße zu erkennen, politisch sensible Inhalte zu blockieren oder für gezielte Werbung, ist rechtlich nicht erlaubt, wenngleich die Technologie zu all diesen Dingen in der Lage ist. Selbst dort, wo DPI erlaubt ist, darf es grundsätzlich nicht willkürlich eingesetzt werden. Europäische Datenschutzgesetze und die EU-Charta der Grundrechte schützen die Vertraulichkeit der Kommunikation. DPI würde auch gegen die Europäische Menschenrechtskonvention verstoßen, da es wahllose Massenüberwachung ohne richterliche Genehmigung bedeutet: Es kann jede Form von Information auslesen, die Computer senden und empfangen. In den USA ist die Lage deutlich anders, da DPI nicht reguliert ist, und viele Unternehmen es für gezielte Werbung nutzen. Wenn Sie etwa E-Mail über Gmail™ oder Yahoo™ nutzen, sind die damit gesendeten und empfangenen Nachrichten mit großer Wahrscheinlichkeit durch amerikanische Netze gereist und somit Gegenstand von DPI. Es stellte sich heraus, dass DPI auch in Verbindung mit den kürzlich aufgedeckten weltweiten Massenüberwachungsprogrammen des US-Geheimdienstes NSA (National Security Agency) und des Britischen Geheimdienstes GCHQ (United Kingdom's General Communications Headquarters) eingesetzt wird.

Wie DPI erkannt, eingegrenzt oder kontrolliert werden kann, ist ein Graubereich. Die Gesetzgebung versucht, mit den technischen Möglichkeiten Schritt zu halten. Es ist sehr schwer feststellbar, in welchem Ausmaß DPI zum Einsatz kommt. Jede Nachricht, die Sie senden, kann quer durchs Netz um die ganze Welt reisen, bevor sie am Zielrechner ankommt. Sie könnte von DPI durch einen Internetprovider genauso betroffen sein wie von staatlichen Sicherheitsbehörden verschiedener Länder. DPI erzeugt auch zusätzliche Informationen, die etwa zwischen Internet Providern und staatlichen Stellen ausgetauscht werden könnten. Es ist sehr schwer zu ermitteln, wo DPI eingesetzt wird, sowie was mit den von DPI produzierten Suchergebnissen passiert. Ohne Regulierung herrscht eine Art „Ausnahmezustand“, in dem Unternehmen und Staaten

gleichermaßen die rechtlichen Grauzonen ausnützen können.

Wir können sagen, dass weltweit viele verschiedene Institutionen DPI einsetzen. Internetprovider, Marketingunternehmen, die Polizei und Sicherheitsbehörden in vielen Ländern nutzen DPI unterschiedlich. Abseits der kürzlich aufgedeckten Massenüberwachungsprogramme (rund um PRISM) gibt es ein paar dokumentierte Fälle. Einige sind kommerziell, andere im Bereich öffentlicher und nationaler Sicherheit.

6.2.1 Kommerzielle Anwendungen

- > **Netzwerksicherheitsmanagement:** Nachrichten werden inspiziert um sicherzugehen, dass sie keine Viren enthalten. Zudem wird beim Austausch großer Dateien häufig gefiltert.
- > **Verhaltensbezogene Werbung:** Aus Nachrichten werden Daten über die Produktvorlieben einer Person gewonnen. In Europa ist diese Werbform nicht erlaubt, allerdings in den USA, und wird von manchen Konsumenten begrüßt. Produkte und Dienstleistungen können so auf ihre (angenommenen) Bedürfnisse hin angeboten werden.
- > **Digitales Rechtemanagement:** Nachrichten werden inspiziert, um illegales Filesharing und Urheberrechtsdelikte zu erkennen.

Kontroverse über Deep Packet Inspection: Phorm und Konsumentendaten in Großbritannien

2008 versuchte das US-Unternehmen Phorm, in England gemeinsam mit Britischen Telekomprovidern (British Telecom, Virgin Media und TalkTalk) ein DPI-System einzuführen. Phorm verwendete DPI um die Surfgewohnheiten von Nutzern zu überwachen. Es analysierte die Daten, die dann an die Werbeindustrie weiterverkauft wurden. Die Provider erzählten den Kunden, die Überwachung werde zum Kampf gegen Cyberverbrechen eingesetzt. Jedoch nicht, dass die Information für Werbezwecke genutzt wird. Die British Telecom testete die Technologie heimlich und führte mehr als 18 Millionen Überwachungen durch. Als die britischen Konsumenten davon erfuhren, protestierten sie dagegen, dass die Daten ohne ihre Zustimmung verwendet wurden. Schließlich wurde die Phorm-Technologie von allen Providern aufgegeben. Die Europäische Kommission leitete rechtliche Schritte gegen die Britische Regierung ein, die den Einsatz genehmigt hatte. Der Fall wurde im Januar 2012 abgeschlossen, als England den Rechtsrahmen um Sanktionen bei illegaler Kommunikationsüberwachung erweiterte.

- > bei denen rassistische Information verbreitet, oder rassistische Bedrohungen gemacht werden
- > bei denen zu Terrorismus angestiftet oder Terrorismus organisiert
- > bei denen Information verbreitet wird, die Völkermord oder Verbrechen gegen die Menschheit gutheißt.

- > **Zensur:** Es wird vermutet, dass DPI von unterdrückenden Regimes weltweit genutzt wird, um politische Gegner zu kontrollieren. Das US-Verteidigungsunternehmen NARUS (eine Tochtergesellschaft von Boeing) verkaufte DPI-Technologie an Libyen, wo sie gegen Dissidenten während des Arabischen Frühlings eingesetzt wurde. Im Gegensatz dazu schränkte England im Zuge jenes Arabischen Frühlings den Verkauf von DPI-Technologie an Ägypten, Bahrain und Libyen durch den Widerruf von Export-Lizenzen ein. Obwohl unklar ist, wer die Technologiezulieferer sind, ist bekannt, dass der Iran DPI nicht nur zur Überwachung der BürgerInnen und Zensur von Online-Information nutzt, sondern auch für gezielte Desinformation durch die Veränderung von Online-Inhalten. China verwendet DPI auf ähnliche Weise. Zudem gibt es eine Reihe ungeklärter Fragen was den Einsatz von Internetzensur in Europa betrifft.

6.2.2 Anwendungen im Bereich der öffentlichen und nationalen Sicherheit

- > **Staatliche Überwachung krimineller Aktivitäten:** Deep Packet Inspection ist als investigatives Werkzeug bei sehr speziellen Verbrechen geplant, obwohl das rechtlich höchst umstritten ist. Das beinhaltet Verbrechen,
 - > die gegen Computersysteme durchgeführt oder mit einem Computer begangen werden (z.B. die Verbreitung von Kinderpornographie)

6.3 Sicherheitsverbesserungen

Deep Packet Inspection kann zu mehr Informationssicherheit und zur Verbrechensbekämpfung beitragen, indem schädliche oder kriminelle Inhalte blockiert werden (wie in Abschnitt 6.2.2 beschrieben).

Obwohl DPI keine schweren Straftaten, auf die sich überwachte Inhalte beziehen, verhindern kann, ist es damit möglich, die präventive Erkennung und die Beweisfindung in Ermittlungen zu unterstützen. Es kann helfen zu verhindern, dass Viren und andere Arten von Cyber-Kriminalität verbreitet werden.

6.4 Kritische Aspekte

Deep Packet Inspection wirft die folgenden schwerwiegenden Fragen auf:

1. 1. DPI ist allumfassend.

- > Es kann sämtliche Nachrichten und Inhalte inklusive aller mitunter enthaltenen sensiblen Daten während der Übertragung analysieren. Das bedeutet, dass mit DPI elektronische Kommunikation nicht mehr privat möglich ist.
- > Zu wissen, dass es keine private Kommunikation mehr gibt, kann zu bedrohlichen Effekten führen. Dem sogenannten ‚Chilling‘ Effekt, bei dem Personen zunehmend Angst haben, frei und offen zu kommunizieren und sie selbst zu sein.
- > DPI ist eine Technologie mit enormer Macht und muss daher sehr eng reguliert werden.

2. Die Regulierung kann kaum mit dem technischen Wandel Schritt halten.

- > Es gibt keine eindeutigen rechtlichen Bestimmungen, wofür DPI eingesetzt und nicht eingesetzt werden darf.
- > In der Praxis hängt das nur von den ethischen Grundsätzen jener ab, die DPI einsetzen. Von der Erkennung von Computerviren zur politischen Unterdrückung kann es für alles verwendet werden.

- > In Ländern, wo nationale Regierungen und Kommunikationsanbieter eng miteinander verwoben sind, kann Information derart gemeinsam genutzt werden, dass der Staat Zugriff auf die gesamte elektronische Kommunikation seiner BürgerInnen hat.

3. Es ist schwer zu sagen, wer genau DPI nutzt, und in welchen Bereichen es eingesetzt wird.

- > Rechtliche Bestimmungen müssten eindeutig und weltweit gültig sein. Seit langem fordern Datenschutzexperten einen weltweiten Mindeststandard für den Schutz der Privatsphäre.
- > Eine „DPI Aufsichts- oder Regulierungsbehörde“ müsste eine absolut zuverlässige internationale Stelle mit genügend Macht sein, um jene, die DPI nicht gesetzeskonform einsetzen, wirksam bestrafen zu können.

4. Die Wirksamkeit von DPI ist fragwürdig

- > Computer erkennen nur möglicherweise problematische Inhalte; es besteht die Gefahr fehlerhafter Interpretation, und dass unschuldige Personen zu Verdächtigen werden.
- > Einige Experten bestreiten die Wirksamkeit von DPI beim Aufspüren illegaler Inhalte.



Viele Unternehmen, die DPI nutzen, haben ihren Sitz außerhalb Europas, analysieren aber Daten über europäische BürgerInnen. Das kann nicht verhindert werden.

Eva Schlehahn, Unabhängiges Landeszentrum für Datenschutz, Schleswig Holstein

7 Smartphone Location Tracking - Handyortung

Wenn Aisha ihr Handy einschaltet, fällt ihr auf, dass sich der auf dem Bildschirm angezeigte Standort geändert hat. Sie war sicher, dass es dafür eine plausible Erklärung gibt. In der Tat müssen alle Mobiltelefone naturgemäß ihren Standort kennen, um zu funktionieren. Smartphones bringen diesen Aspekt aber auf eine völlig neue Ebene.

Das Smartphone ist als multifunktionales Werkzeug und Spielzeug beinahe eine Art digitales Schweizer Taschenmesser geworden. Es gibt rund 5 Milliarden Mobiltelefone weltweit. Im Durchschnitt sind das in Europa rund 1,3 Telefone pro Person. Diese Zahl ist enorm wenn man bedenkt, dass es Mobiltelefone erst seit Anfang der 90er Jahre gibt.

7.1 Warum Smartphone Location Tracking entwickelt wurde

Smartphones sind eine relativ neue Entwicklung. Ihre hohe Beliebtheit verdanken sie ihren vielfältigen Anwendungsmöglichkeiten neben der üblichen Funktion als herkömmliches Mobiltelefon. Smartphones sind eher kleine Taschencomputer, die auch als Telefon verwendbar sind. Wie ein Desktop-PC oder Laptop, haben Smartphones ein eigenes Betriebssystem mit Nachrichten- und E-Mail-Funktion und zum Surfen im Internet. Smartphones bieten vielfältige Softwareanwendungen wie etwa Spiele, Navigationsanwendungen, Nachrichtendienste, etc. Sie beinhalten auch Digital- und Videokameras, sowie Multimediaanwendungen, und haben größere, farbige Displays meist mit Touchscreen-Funktion.

Die Geschichte von Mobiltelefonen reicht zurück bis zum Zweiten Weltkrieg. Ein herkömmliches Mobiltelefon ist im Grunde ein kabelloses Funkgerät zum Senden und Empfangen von Nachrichten. Die ersten Funkgeräte, 'Walkie Talkies', wurden eingeführt, um mit Soldaten an der Front in Kontakt bleiben zu können. In den 1970er und 1980er Jahren wurden die ersten Mobiltelefone entwickelt. Die allerersten Mobiltelefone hatten die Größe und das Gewicht eines Ziegels und der Akku hielt nur 20 Minuten. Wie sich die Zeiten

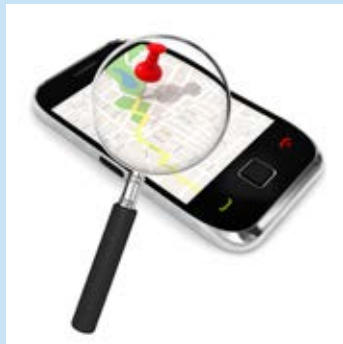
verändert haben! Von den 1980er Jahren bis jetzt hat ein wachsendes Netzwerk an Mobilfunkmasten die Qualität von Telefonverbindungen örtlich und auch über längere Distanzen verbessert. Vielleicht können Sie sich noch daran erinnern, wie Mitte der 1990er deutlich mehr Funkmasten aufgestellt wurden. Als Folge gab es viele Debatten über die Standorte der eher unschönen Masten sowie Gesundheitsbedenken aufgrund der davon ausgehenden Strahlung.



Funkmasten sind wesentlich für die Verortung von Mobiltelefonen. Ein Mast deckt ein bestimmtes geographisches Areal ab. Um sich ins Netz zu verbinden, zu telefonieren und Nachrichten zu senden, müssen sich alle Mobiltelefone am nächstgelegenen Mast registrieren und mit ihm in Verbindung bleiben. Der Mast mit dem eine Verbindung besteht, zeichnet immer den Standort eines Telefons auf. Wenn sich die Person bewegt und in die Zone eines anderen Mastes gelangt, registriert sich das Handy dort. Auf diese Weise erfasst der Mobilfunkbetreiber die Bewegungen eines Handynutzers. Nach derzeit geltendem Recht in der EU sind die Betreiber verpflichtet, diese Daten für mindestens 6 bis 24 Monate zu speichern. Smartphones können zusätzlich dazu auch auf andere Arten lokalisiert werden: Die meisten Telefone bieten etwa GPS Anwendungen oder können sich mit drahtlosen Netzwerken (WLAN, Bluetooth etc.) verbinden. Dabei wird auch die Position bekanntgeben.

Das führte zu einem enormen Zuwachs an sogenannten „Location-based Services“ (standortbasierte Dienste) für Smartphones. Diese sind meist als Mikroanwendungen (sog. „Apps“) verfügbar, die auf dem Telefon installiert werden können. Eine App ist eine Software, die spezielle Funktionen anbietet. Standortbasierte Apps bieten u.a. Informationen zu nahegelegenen Restaurants, Geschäften oder bekannten Personen in der Umgebung. Zudem gibt es auch standortbasierte

Spiele. Standortbasierte Anwendungen werden in den nächsten Jahren voraussichtlich noch weiter zunehmen.



Wie Handyortung funktioniert

Sowohl bei herkömmlichen, als auch „smarten“ Mobiltelefonen ist eine Standorterfassung durchführbar. Es gibt verschiedene Möglichkeiten: über die Mobilfunkmasten, GPS oder kabellose Netzwerke. Die erste Variante funktioniert bei allen Mobiltelefonen, die beiden anderen nur bei Smartphones.

Mobilfunkmasten: Alle Telefone registrieren sich bei dem nächstgelegenen Mast, um Telefonie, SMS und E-Mail über das Mobilfunknetz zu ermöglichen. Jedes Telefon hat eine eindeutige Kennung, die das Telefon einem Benutzerkonto beim Mobilfunkbetreiber zuordnet. Diese Information wird u.a. für die Bereitstellung der Funktionalität an sich und für die Gesprächsabrechnung benötigt. Wenn Sicherheitsorgane oder Strafverfolgungsbehörden herausfinden wollen, wo sich eine Person zu einer bestimmten Zeit aufgehalten hat, können sie die entsprechenden Daten von Mobilfunkbetreibern anfordern. Die Aufzeichnungen des Sendemastes zeigen, ob das Handy einer Person in der Reichweite eines bestimmten Mastes war. Sind die Aufzeichnungen aller Masten verfügbar – wie in der EU vorgeschrieben – können der Handystandort verfolgt, und so die Bewegungen des Benutzers aufgedeckt werden.

GPS: Smartphones beinhalten oft Navigationssoftware und Anwendungen, die GPS benötigen. Wenn GPS am Smartphone aktiviert ist, wird die genaue Position des Telefons berechnet. Das geschieht über Datenaustausch mit GPS-Satelliten. Wenn GPS deaktiviert ist, kann das Handy den Standort nicht per GPS ermitteln. Allerdings kann diese Funktionalität auch ohne Wissen des Nutzers aus der Ferne aktiviert werden. Beispielsweise wenn eine App installiert ist, welche die Ortung im Verlust- bzw. Diebstahlfall ermöglichen soll. App-Anbieter erfassen Standortdaten und einige verkaufen sie für Werbezwecke weiter. Wenn Sicherheitsorgane und Strafverfolgungsbehörden eine bestimmte Person überwachen, können sie auch diese GPS-Daten anfordern.

Wireless (Drahtlos): Smartphones können sich mit drahtlosen Netzen verbinden die in einem bestimmten Areal verfügbar sind. Bei der Verbindung wird das Handy im räumlichen Bereich des Netzes geortet. Auch hier lässt sich die Standorterfassung durch das Abschalten der Drahtlos-Funktion unterbinden. WLAN hat in Gebäuden üblicherweise eine Reichweite von ca. 20 Metern, im Freien auch darüber hinausgehend.

Andere ‚smarte‘ mobile Geräte, wie iPads, Tablet-PCs oder Notebooks mit den entsprechenden Funktionalitäten können auf die gleiche Art und Weise überwacht werden.

Standortbasierte Dienste bieten Smartphone-BenutzerInnen viele Möglichkeiten. Allerdings ist die Menge der dabei offengelegten Informationen aus Sicht von Datenschützern besorgniserregend. Ein anschauliches Beispiel lieferte der deutsche Politiker der Grünen Malte Spitz, der versuchte, die ihn betreffenden Standortdaten seines Mobiltelefons zu erhalten, welche für 6 Monate gespeichert wurden. Dazu musste er die Telefongesellschaft verklagen. Auf den ersten Blick erschienen die Daten wenig aussagekräftig. Doch mit statistischer Analyse der Daten wurde ein sehr detailliertes Bild seines Lebens sichtbar. In Kooperation mit der deutschen Zeitung „Die Zeit“ produzierte Malte eine Animation, die sehr genau zeigte, wo er sich innerhalb dieser 6 Monate aufhielt. Für Malte war der hohe Detailgrad der Informationen besorgniserregend. Insbesondere durch die Kombination der Bewegungsinformation mit Informationen sozialer Medien wie Twitter oder Facebook.

In einem aktuellen Fall des Obersten Gerichtshofs in den USA (United States vs. Jones) stellte der Richter fest, dass GPS Daten dazu in der Lage sind, unbestritten private Aufenthalte, wie etwa in der Psychiatrie, in Schönheitskliniken, Abtreibungskliniken, AIDS Zentren, Strip Clubs, beim Strafverteidiger, in Stundenhotels, bei Gewerkschaftstreffen, in Moscheen, Synagogen oder Kirchen, Schwulenclubs und mehr, zu offenbaren.

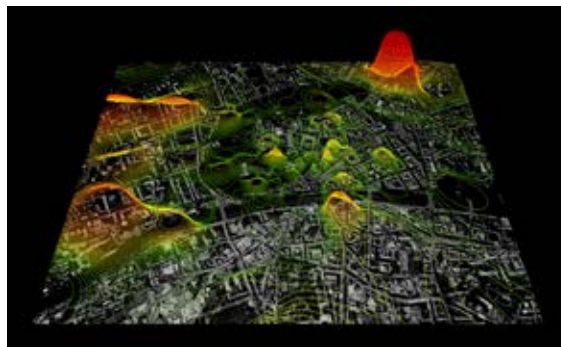
- > **Gezielte Werbung:** Softwareunternehmen, die Apps anbieten, wie Twitter, Angry Birds oder FourSquare, erheben den Standort und andere Kontaktdaten der Handys und verkaufen sie an Werbeunternehmen. Diese nutzen die Daten dann unter anderem, um gezielt Werbung zu platzieren. Angry Birds etwa wurde weltweit eine Milliarde Mal heruntergeladen. Die Benutzer waren überrascht als sich herausstellte, dass die Finnische Entwicklungsfirma (Rovio Entertainment Ltd.) die Standortdaten der Spieler regelmäßig sammelte und weiterverkaufte. Fünfzig Prozent aller Apps sammeln Standortdaten selbst dann, wenn diese für die Anwendung gar nicht benötigt werden.
- > **Stadt- und Regionalplanung:** Standortdaten können eingesetzt werden, um die Nutzung öffentlicher Flächen in Städten abzubilden. Da es in Ballungszentren mehr Handymasten gibt als in ländlichen Regionen, können Handys viel genauer verfolgt werden. Das eher gespenstisch anmutende Bild unten zeigt eine Karte der Handynutzung in Graz. Forscher des renommierten US Technologie-Instituts in Massachusetts (MIT) werteten Mobilfunkdaten anonym aus um zu zeigen, wie sich Menschen durch Graz bewegen. Ziel dieser Karte ist es, Städteplanern Informationen über die Nutzung der Stadt zu liefern.

7.2 Wie Smartphone Location Tracking eingesetzt wird

Es gibt sowohl im kommerziellen als auch im Sicherheitsbereich Verwendung für die Standortdaten von Mobiltelefonen.

7.2.1 Kommerzielle Anwendungen

- > **Verwaltung von Telefonrechnungen:** Mobilfunkbetreiber benötigen die Standortdaten und die Kennung des Telefons zur Bereitstellung der Dienste und zur Kostenabrechnung.



7.2.2 Anwendungen im Bereich öffentliche und nationale Sicherheit

- > **Auffinden vermisster und verletzter Personen:** In den USA und Kanada gibt es einen Dienst namens E-911 (Enhanced 911), welcher die Verwendung von GPS in allen Mobiltelefonen im Falle der Absetzung eines Notrufs zulässt, damit die Telefone (und ihre Nutzer) in einem Notfall geortet werden können. In Europa werden jährlich ca. 180 Millionen Notrufe getätigt. 60 bis 70 % dieser Notrufe stammen von Mobiltelefonen. Das Telefon übermittelt den Aufenthaltsort an die europaweite Notrufnummer 112. Im Gegensatz zu Amerikanern und Kanadiern sind Europäer nicht verpflichtet, bei einem Notruf vom Handy aus immer GPS mit zu aktivieren.
- > **Bewegungsverfolgung von Verdächtigen:** Sicherheits- und Strafverfolgungsorgane sind mittels Anfragen an Mobilfunkbetreiber in der Lage, auf standortbasierte Daten zuzugreifen. Derzeit sind solche Anfragen in Europa rechtlich geregelt. Nach Eingang einer solchen Anfrage sind Unternehmen verpflichtet, die angeforderten Daten über Verdächtige zu übermitteln. Sicherheitsorgane haben daneben auch andere Methoden, um Telefone zu überwachen, die bei bestimmten Zielpersonen eingesetzt werden können.
- > **Überwachung von Familienmitgliedern:** Einzelne Nutzer könnten auch im privaten Bereich von standortbasierten Diensten Gebrauch machen. Viele Eltern werden mit individuellen Produkten zur Mobiltelefonortung vertraut sein, die es etwa ermöglichen, den Standort ihrer Kinder jederzeit festzustellen.

Kontroversen bei Smartphone Location Tracking

Als Folge der „Occupy“ Bürgerprotestbewegungen in New York wurde Twitter gezwungen, Standortdaten an die US-Regierung zu übermitteln, um die DemonstrantInnen zu identifizieren. Kürzlich startete Twitter einen neuen Dienst namens „Please Don’t Stalk Me“ (Bitte stalke mich nicht). Das ermöglicht BenutzerInnen, ihre Standortdaten zu verschleiern, die an ihre Tweets gekoppelt sind. Diese Anwendung lässt NutzerInnen jeden beliebigen Standort auf der Welt mittels Google Maps festzulegen und in ihre Tweets einbinden. Andere Apps wie „My Fake Location“, „Fake GPS Location“ und „GPS Cheat“ funktionieren ähnlich.

7.3 Verbesserungen der Sicherheit

Handyortung kann die Sicherheit auf verschiedene Arten erhöhen:

1. Sie ermöglicht jenen, die sich in Notsituationen befinden, gefunden zu werden und Hilfe zu erhalten.
2. Sie unterstützt Angehörige bei der Beobachtung von hilfsbedürftigen Personen oder Kindern.
3. Die Polizei und Strafverfolgungsbehörden können die Standortdaten verwenden um festzustellen, ob Personen an Tatorten waren, oder um Verdächtige auszuschließen. Sie können auch Verdächtige bei laufenden Ermittlungen überwachen.

7.4 Kritische Aspekte

Handyortung wirft kritische Fragen im Zusammenhang mit Datenschutz, Regulierung und Grundrechten auf:

1. AnwenderInnen haben keine vollständige Kontrolle über die Informationen, die ihr Smartphone weitergibt. Das ist vor allem schwierig für gefährdete Personen, wie geschützte Zeuginnen, die ihre Standortdaten nicht preisgeben wollen, aber trotzdem mobil telefonieren möchten. Einige Telefone wie iPhones speichern automatisch Standortdaten ohne dass sich dies deaktivieren lässt.
2. Einige Apps sammeln Standortdaten selbst dann, wenn diese für die Nutzung gar nicht benötigt werden. Ohne starken Druck aus der Öffentlichkeit ist es unwahrscheinlich, dass Unternehmen den KonsumentInnen mehr Kontrolle über ihre Daten geben.
3. Viele App-Anbieter haben ihren Sitz außerhalb von Europa und sind daher nicht an Europäische Datenschutzgesetze gebunden. Für die EU ist es deshalb schwierig, Privatsphäre-freundliche Anwendungen zu fordern. Allerdings verlangt eine kürzlich verabschiedete Novelle der E-Privacy-Richtlinie auf europäischer Ebene, dass die Zustimmung der Nutzer erforderlich ist, wenn Standortdaten verarbeitet werden, egal in welchem Land die Anbieter angesiedelt sind.
4. Ähnlich wie bei Deep Packet Inspection könnten Informationen von nationalen Regierungen und privaten Diensteanbietern gemeinsam genutzt werden, so dass der Staat Zugang zu den Standortdaten aller BürgerInnen erhält.
5. Da Standortdaten eingesetzt werden können, um Demonstranten zu identifizieren, besitzt schon die mögliche Verwendung der Daten einen potenziell abschreckenden Effekt, da BürgerInnen von der Teilnahme an Demonstrationen vielleicht absehen und von der Ausübung ihrer demokratischen Grundrechte abgehalten werden könnten.



Handyortung verleiht Menschen Möglichkeiten, ebenso wie sie Menschen überwacht. Sie kann eine Reihe von Diensten ermöglichen und soziale Beziehungen verbessern...aber die Konfigurationseinstellungen zur Nutzung von Standortdaten sind nicht immer einleuchtend und nicht einfach zu verstellen.

Gus Hosein, Privacy International

8 Ist Technik die einzige Antwort?

Sie fragen sich vielleicht, ob Sicherheitstechnologien die einzige Antwort auf Sicherheitsprobleme sind. Zur Zeit hat es den Anschein, als wäre die Überwachung und die Identifikation von Verdächtigen aus dem Kreis der allgemeinen Bevölkerung das Einzige, worum es bei Sicherheit geht. Das ist zwar teilweise der Fall, doch nicht die ganze Geschichte.

Die zuvor erwähnten europäischen Sicherheitsziele scheinen nahezulegen, dass Sicherheit etwas ist, das alle Lebensbereiche umfasst. Sie betreffen zumeist die ‚klassischen‘ Sicherheitsaspekte wie Verbrechen und Terrorismus. Wie auf den vorherigen Seiten gezeigt wurde, ist es möglich, neue Sicherheitstechnologien zu nutzen, um Personen zu identifizieren, die an solchen Aktivitäten beteiligt sind. Aber es gibt tieferliegende Ursachen, aus denen Sicherheitsprobleme entstehen, wie etwa Armut, nationale oder internationale Konflikte, sowie politische und religiöse Differenzen. Sicherheitstechnologien sind nicht in der Lage, diese Grundprobleme zu lösen.

Europäische Sicherheitszielsetzungen sprechen auch von Sicherheitsproblemen, wenn es sich um Krisen oder Katastrophen handelt. Diese Katastrophen können Nahrungs- oder Wasserknappheit, Finanzkrisen, die Verbreitung von Seuchen oder Naturkatastrophen sein: Situationen die die menschliche Sicherheit insgesamt herausfordern. Auch hier sind Sicherheitstechnologien wenig effektiv bei der Bewältigung von solchen längerfristigen, komplexeren Sicherheitsproblemen.

Während Sicherheitstechnologien also eingesetzt werden, um Kriminelle und Terroristen zu finden und zu versuchen, ihre nächsten Schritte vorherzusehen, gibt es auch andere Lösungen. Wir haben einige davon hier folgend aufgelistet. Vielleicht haben Sie selbst auch einige Ideen, wie Sicherheit verbessert werden kann. Oder vielleicht denken Sie, dass der Sicherheitsfokus in Europa weniger stark auf Verbrechen und Terror liegen, sondern sich anderen Prioritäten zuwenden sollte.

8.1 Regionale Lösungen

- > Förderung einer sicher gestalteten Umgebung durch verbesserte Straßenbeleuchtung, Notfalltelefone und verstärkte Polizeipräsenz
- > Verbesserung kommunaler Nachbarschaftsbeziehungen und Kooperationen mit der Polizei durch gemeinschaftliche Maßnahmen zur Verbrechensprävention
- > Lokale, religiöse oder andere Vereine könnten Probleme selbst lösen und dadurch dazu beitragen, daß der soziale Zusammenhalt gestärkt wird
- > Transparente und verantwortungsvolle regionale Verwaltung und Polizeiarbeit
- > Schaffung eines breiten Angebots an Arbeit, Ausbildung und Betreuung für jene, die gefährdet sind, mit Kriminalität in Berührung zu kommen

8.2 Nationale oder internationale Lösungen

- > Förderung fairer globaler Systeme für Handel, Entwicklungshilfe und Schuldenabbau
- > Verbesserung von Katastrophenschutzinfrastruktur und Ressourcen
- > Verbesserung der Wasser-, Informations- und Kommunikationsinfrastruktur sowie Lebensmittelversorgung in bedürftigen Regionen
- > Effizientere Nutzung nachhaltiger und alternativer Energiequellen
- > Lösungen für Probleme, die durch Ungleichheit und Diskriminierung entstehen

9 Nun zu Ihnen...

Wir hoffen, dass Sie sich mit dieser Information nicht überfordert fühlen! Die gute Nachricht: Sie haben nun das Ende dieser Broschüre erreicht und können sich Zeit nehmen, über die Dinge nachzudenken, die hier angesprochen wurden.

Wir haben drei Sicherheitstechnologien gezeigt, die wir in den BürgerInnen-Foren diskutieren werden. Wir haben erläutert, wie diese funktionieren, wie sie verwendet werden, welche Sicherheitsverbesserungen sie ermöglichen und welche kritischen Aspekte sie aufwerfen. Wir haben auch erläutert, in welchem Zusammenhang diese Technologien entwickelt werden: In einem Europa, das sehr um Sicherheit besorgt ist, und wo Sicherheit ein Teil des täglichen Lebens ist. Kritische Aspekte zu Überwachung und Privatsphäre sind durch die Vielzahl an persönlichen Daten, die zu Sicherheitszwecken verwendet werden, ebenso bedeutend. Schließlich haben wir alternative, nicht-technische Ansätze betrachtet, um Sicherheit in der Gesellschaft zu gewährleisten.

Nun liegt es an Ihnen, sich Ihre Meinung zu diesen Dingen zu bilden. Wenn diese Technologien alltäglich für Sicherheitszwecke eingesetzt werden, wie akzeptabel ist das? Vielleicht meinen Sie, dass jede Technologie auf ihre eigene Weise effektiv bei der Erhöhung der Sicherheit ist und eventuell Verbrechen reduzieren kann. Aber vielleicht meinen Sie auch, dass alternative, nicht-technische Lösungen besser wären. Vielleicht sind Sie der Ansicht, dass klassische Methoden mit ausgebildeten Sicherheitsorganen oder Polizei eher angewendet werden sollten als weitreichende Informationsüberwachung. Vielleicht denken Sie auch, dass Sicherheit kein so großes Problem ist und wir uns nicht zu viel Sorgen machen sollten.

Genauso vertrauen Sie vielleicht darauf, dass diese Technologien in sicheren Händen sind, weil die staatlichen Stellen, die sie nutzen, öffentlich verantwortlich sind. Oder vielleicht haben Sie Zweifel, inwieweit diese Behörden in der Lage sind, die Sicherheitstechnologien kompetent, verantwortungsbewusst und zum Wohle der Gesellschaft einzusetzen.

Vielleicht haben Sie das Gefühl, diese Technologien betreffen Sie nicht wirklich: Letztlich sind sie auf andere gerichtet, die etwas falsch gemacht haben und werden ohnehin in Plätzen oder Orten eingesetzt, wo sie sich nicht aufhalten. Aber möglicherweise sind Sie der Meinung, dass sich jeder über diese Dinge Gedanken machen sollte, da diese Technologien sehr viele Daten verarbeiten und jeden zu einem potenziellen Verdächtigen machen. Vielleicht haben Sie kein Problem damit, wie Sicherheitstechnologien heute eingesetzt werden, aber vielleicht sind Sie besorgt, wie das in Zukunft aussehen könnte.

Was immer Sie auch denken, ein wenig Privatsphäre gegen etwas mehr Sicherheit einzutauschen, ist für niemanden eine leichte Entscheidung. SurPRISE möchte die verschiedenen Meinungen und Sichtweisen verstehen, welche die Menschen zu neuen Sicherheitstechnologien haben.

Wir freuen uns sehr darauf, Sie in wenigen Wochen beim BürgerInnen-Forum begrüßen zu dürfen. Wenn Sie mehr über das Projekt und die beteiligten Institutionen erfahren möchten, besuchen Sie gerne auch die offizielle (englischsprachige) SurPRISE Homepage unter <http://surprise-project.eu> oder kontaktieren Sie uns.

Über dieses Dokument

Diese Informationsbroschüre wurde hergestellt, um die Personen zu informieren, die am BürgerInnen-Forum des SurPRISE Projekts teilnehmen. Diese Publikation wird vom Institut für Technikfolgen-Abschätzung (ITA, an der Österreichischen Akademie der Wissenschaften, Strohgassee, 45/5, 1030 Wien) allen Partnern im SurPRISE Konsortium zur Verfügung gestellt. Lesen Sie mehr über das Projekt und die Partner auf der (englischsprachigen) SurPRISE Website: <http://surprise-project.eu/>.

Die Information in dieser Broschüre stammt aus Berichten, die von SurPRISE Projektmitarbeitern geschrieben wurden, auf der Basis von internationalen wissenschaftlichen Forschungsarbeiten und der Arbeit von politischen Entscheidungsträgern sowie Technologieentwicklern.

- > **Autorin:** Dr Kirstie Ball, The Open University
- > **Wissenschaftlicher Beirat:** Dr. Monica Areñas Ramiro, Robin Bayley, Prof. Colin Bennett, Dr. Gloria González Fuster, Dr. Ben Hayes, Dr. Majtényi László, Jean Marc Suchier, Nina Tranø, Prof. Ole Wæver
- > **Layout:** Peter Devine, David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University; Jaro Sterbik-Lamina, ITA/ÖAW
- > **Bilder:** David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University.
Page 17 © iStockPhoto.com / EdStock,
page 28 © iStockPhoto.com / dpmike,
page 29 © iStockPhoto.com / alexsl,
page 30 Senseable City Lab, Massachusetts Institute of Technology.
- > **SurPRISE sponsors:** European Commission Framework 7 Programme, project no. 285492
- > Diese Broschüre ist online verfügbar unter: <http://surprise-project.eu>
- > **Wie dieses Dokument hergestellt wurde:** Diese Informationsbroschüre wurde von Kirstie Ball in enger Kooperation mit der Danish Board of Technology Foundation, dem SurPRISE Konsortium und seinem Beirat verfasst. Die Broschüre wurde vier internen und einem externen Begutachtungsverfahren unterzogen, und wurde mit Bürgergruppen in Dänemark, Ungarn und Großbritannien getestet.

Projekt-Partner

- > Institut für Technikfolgen-Abschätzung/Österreichische Akademie der Wissenschaften, Koordinator, Österreich (ITA/ÖAW)
- > Agencia de Protección de Datos de la Comunidad de Madrid*, Spanien (APDCM)
- > Instituto de Políticas y Bienes Públicos/Agencia Estatal Consejo Superior de Investigaciones Científicas, Spanien (CSIC)
- > Teknologirådet - The Danish Board of Technology Foundation, Dänemark (DBT)
- > European University Institute, Italien (EUI)
- > Verein für Rechts-und Kriminalsoziologie, Österreich (IRKS)
- > Medián Opinion and Market Research Limited Company, Ungarn (Median)
- > Teknologirådet - The Norwegian Board of Technology, Norwegen (NBT)
- > The Open University, Vereinigtes Königreich (OU)
- > TA-SWISS/Akademien der Wissenschaften Schweiz, Schweiz (TA-SWISS)
- > Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein/Deutschland (ULD)

* APDCM, die Agencia de Protección de Datos de la Comunidad de Madrid (Datenschutzbehörde der Stadtgemeinde Madrid) war bis zum 31. Dezember 2012 Partner im SurPRISE Konsortium. Auf Grund der Sparpolitik in Spanien wurde sie mit Ende 2012 geschlossen.

Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe.

(Überwachung, Privatsphäre und Sicherheit: Ein großflächiges Beteiligungsverfahren zur Bewertung von Kriterien und Faktoren für Akzeptabilität und Akzeptanz von Sicherheitstechnologien in Europa.)



