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

Projektkürzel: **SurPRISE**

Gemeinschaftliches Projekt

Grant Agreement Nr.: 285492

FP7 Call Thema: SEC-2011.6.5-2: The Relationship Between Human Privacy And Security

Start des Projekts: Februar 2012

Dauer: 36 Monate

D 6.3 – Bürgerforen zum Thema Privatsphäre, Sicherheit und Überwachung: Länderreport Deutschland

Lead Beneficiary: ULD

Autor(en): Eva Schlehahn (ULD)

Veröffentlichungsstatus: Öffentlich

Version: 1

Dieses Projekt wird durch das 7te Rahmenprogramm der Europäischen Union für Forschung, technische Entwicklung und Demonstration unter dem Grant Agreement Nr. 285492 gefördert.

Dieses Dokument wurde durch das SurPRISE Projekt (http://www.surprise-project.eu) erstellt, mitgefördert innerhalb des siebten Rahmenprogramms (FP7). SurPRISE untersucht das Verhältnis zwischen Sicherheit und Privatsphäre. SurPRISE wird neue Einsichten in das Verhältnis von Überwachung, Privatsphäre und Sicherheit bieten, unter Einbeziehung der Sichtweise Europäischer Bürger als zentrales Element. Ferner werden Optionen für die Privatsphäre weniger beeinträchtigende Sicherheitstechnologien und nichttechnische Sicherheitslösungen erforscht mit dem Ziel, informierte Debatten in Bezug auf Sicherheitsstrategien zu ermöglichen.

Das SurPRISE Projekt besteht aus einem Konsortium mit den folgenden Partnern:

Institut für Technikfolgen-Abschätzung / Österreichische Akademie der Wissenschaften Coordinator, Austria	ITA/OEAW	
Agencia de Protección de Datos de la Comunidad de Madrid*, Spain	APDCM	
Instituto de Politicas y Bienes Publicos/ Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain	CSIC	
Teknologirådet - The Danish Board of Technology Foundation, Denmark	DBT	
European University Institute, Italy	EUI	
Verein für Rechts-und Kriminalsoziologie, Austria	IRKS	
Median Opinion and Market Research Limited Company, Hungary	Median	
Teknologirådet - The Norwegian Board of Technology, Norway	NBT	
The Open University, United Kingdom	OU	
TA-SWISS / Akademien der Wissenschaften Schweiz, Switzerland	TA-SWISS	
Unabhängiges Landeszentrum für Datenschutz, Germany	ULD	

This document may be freely used and distributed, provided that the document itself is not modified or shortened, that full authorship credit is given, and that these terms of use are not removed but included with every copy. The SurPRISE partners shall all take no liability for the completeness, correctness or fitness for use. This document may be subject to updates, amendments and additions by the SurPRISE consortium. Please, address questions and comments to: feedback@surprise-project.eu

*APDCM, die Agencia de Protección de Datos de la Comunidad de Madrid (Datenschutzaufsichtsbehörde der Kommune Madrid) nahm bis zum 31. Dezember 2012 als Konsortium Partner am SurPRISE Projekt teil.

Aufgrund einer Neustrukturierung der Datenschutzbehörden in Spanien wurde die Teilnahme von APDCM am Projekt Ende des Jahres 2012 beendet.

Inhaltsverzeichnis

Zusammenfassung

SurPRISE überprüft das Verhältnis zwischen Sicherheit und Privatsphäre, oftmals wird dies als eine Abwägung zwischen den beiden wahrgenommen (im Englischen zumeist als "trade-off" bezeichnet). Wann immer Sicherheitsmaßnahmen und Technologien auf die Sammlung von Informationen über Bürgerinnen und Bürger[1] gerichtet sind, steht die Frage im Raum, ob und bis zu welchem Grad deren Privatsphäre verletzt wurde. Diese Verletzung der individuellen Privatsphäre wird manchmal als ein akzeptabler Preis zugunsten verbesserter Sicherheit gesehen. Entsprechend wird angenommen, dass Bürger bereit sind, ihre Privatsphäre aufzugeben um ein Mehr an persönlicher Sicherheit in unterschiedlichen Lebensbereichen zu gewinnen. Dieses verbreitete Verständnis des Sicherheit-Privatsphäre Verhältnisses sowohl aus staatlicher, wie auch aus Bürgersicht, hat sowohl politische Entscheidungsträger, Gesetzgebungsprozesse und Best Practice Anleitungen in Bezug auf die Sicherheitspolitik innerhalb der Europäischen Union geprägt.

Gleichwohl zweifeln neuere Arbeiten die Allgemeingültigkeit dieses Sicherheit-Privatsphäre Trade-Offs an. Jene Arbeiten legen nahe, dass in diesem Modell die Auswirkungen von Sicherheitsmaßnahmen auf Bürger in Bezug auf aktuelle Sicherheitspolitik und entsprechende Praktiken zu stark vereinfacht berücksichtigt würden. Aus diesem Grund würden die tiefergehenden komplexen Fragestellungen von Privatsphäre bezogenen Bedenken und die öffentliche Skepsis hinsichtlich überwachungsorientierten Sicherheitstechnologien (im Folgenden zugunsten besserer Lesbarkeit verkürzt: Sicherheitstechnologien) nicht deutlich genug für rechtliche und technische Experten.

Als Antwort auf diese Entwicklungen hat das SurPRISE Projekt direkt Bürger in neun EU Mitgliedsstaaten und verbundenen Staaten[2] hinsichtlich des "security-privacy trade-off" befragt. Diese konnten in Bürgerforen verschiedene Sicherheitstechnologien und Maßnahmen betrachten.

Dieses Deliverable präsentiert die Ergebnisse des SurPRISE Bürgerforums zu Sicherheit, Privatsphäre und Überwachung, welches im März 2014 in Kiel, ausgerichtet wurde. Während dieser Veranstaltung wurden die Sichtweisen und Meinungen der teilnehmenden Bürger hinsichtlich Sicherheit, Privatsphäre und speziell vorausgewählten, beispielhaften Sicherheitstechnologien erforscht.

Der Zweck dieses Bürgerforums ist es, Einblick in die Meinungen der Teilnehmer zu diesen Themen zu gewinnen, um die Auswirkungen und Bedenken hinsichtlich der Sicherheitspolitik und Praxis der EU aus der Sicht europäischer Bürger zu untersuchen. Das Ziel ist es, Forschungsergebnisse für politische Entscheidungsträger zusammenzutragen, die mit der Gestaltung der zukünftigen Sicherheitsstrategie in Europa und den entsprechenden Regelwerken betraut sind. Zusammen mit der zusätzlichen Forschungsarbeit des SurPRISE-Projekts können die Ergebnisse des Bürgerforums europäischen Entscheidungsträgern Hinweise geben, welche Fragestellungen zwingend in Angriff genommen werden müssen. Insbesondere betrifft dies die Voraussetzungen, unter denen die Nutzung von Sicherheitstechnologien von Bürgern akzeptiert werden, unter Einbeziehung der bedeutsamsten Hürden in Zusammenhang mit Grundrechten und demokratischen Grundprinzipien in Europa.

Oft wird das Verhältnis von Sicherheit und Privatsphäre als eine notwendige Balance gesehen, um ein Mehr an Sicherheit zu erreichen. Diese Auffassung hat die Gesetzgebung und die Praxis über Jahre hinweg stark beeinflusst. Jedoch legt die öffentliche Diskussion, insbesondere angetrieben durch die neueren NSA-Enthüllungen, nahe, dass das klassische Trade-Off Modell einen zu kurz gesprungenen Blick auf das Sicherheit/Privatsphäre Verhältnis bietet. Es wurde deutlich, dass trotz geforderten Erfolgen im Sicherheitsbereich, die Privatsphäre und Menschenrechte allgemein europaweit eine wichtige Rolle in Bezug auf den sicherheitspolitischen öffentlichen Diskurs spielen. Die Bedenken legen nahe, dass die Angelegenheit komplexer ist als

[1] Im Folgenden wird zur besseren Lesbarkeit des Dokuments nur die männliche Sprachform benutzt. Gemeint sind aber sowohl Bürgerinnen wie auch Bürger.

[2] Österreich, Dänemark, Deutschland, Ungarn, Italien, Norwegen, Spanien, die Schweiz, und Großbritannien.

die simple Annahme, dass europäische Bürger ohne weiteres mit dem bedingungslosen Tausch von individueller Privatsphäre gegen Sicherheitsvorteile einverstanden seien.

Das SurPRISE-Projekt hat diese Bedenken als Antwort auf aktuelle Entwicklungen mittels der Durchführung der eingangs erwähnten Bürgerforen in neun verschiedenen EU-Mitgliedstaaten und verbundenen Staaten adressiert. Mit durchschnittlich 200 Teilnehmern pro Land zielten die Bürgerforen darauf ab, die Sichtweisen der Bürger auf das Sicherheit-Privatsphäre Verhältnis zu erforschen, während diese vorausgewählte überwachungsbasierte Sicherheitstechnologien diskutierten. Bei dem deutschen Bürgerforum hatten die Teilnehmer die Chance, ihre Meinung in Bezug auf die beiden ausgewählten Technologien Intelligente Videoüberwachung (Smart CCTV) und Handyortung (Smartphone Location Tracking) kund zu tun. Dieses Deliverable stellt die Ergebnisse dieses Bürgerforums in Deutschland auf nationaler Ebene vor.

In diesem Dokument werden in Kapitel 2 die Ergebnisse zunächst in einen nationalen Kontext für Deutschland gesetzt. Hierbei wird die aktuelle Situation, entstanden aus dem historischen Hintergrund des Landes, beleuchtet. Heutzutage ist die Staatsstruktur Deutschlands eine parlamentarische Demokratie. Jedoch ist das Land noch immer unter dem Eindruck der Ereignisse der Vergangenheit unter den repressiven Regimes der Nationalsozialisten unter Hitler und der Deutschen Demokratischen Republik (DDR). Die Erfahrungen dieser beiden repressiven Regimes und die gesellschaftliche Zersetzung, hervorgerufen durch die intensiven Spionagetätigkeiten der nationalsozialistischen Geheimpolizei und des DDR Staatssicherheitsdienstes (Stasi), hat ein tiefes Misstrauen deutscher Bürger gegenüber staatlicher Überwachung für Sicherheitszwecke hinterlassen. Dieses Misstrauen hat sich zunächst infolge der terroristischen Anschläge vom 11. September 2001 und der Folgeereignisse verringert. Es kehrte jedoch zusehends zurück in die öffentliche Wahrnehmung und befeuerte einen kontroversen medialen Diskurs nach den Enthüllungen des Whistleblowers Edward Snowden über die Spionageaktivitäten der NSA. Dies ist die Ausgangssituation für die folgenden Abschnitte, welche die wichtigsten Aspekte deutscher Sicherheitspolitik und Sicherheitsstrategien, die entsprechenden Fragen in Bezug auf Privatsphäre, die öffentliche Diskussion über Sicherheitstechnologien und die mit diesen verbundene Praxis erläutern.

Mit diesem Hintergrund wurde das deutsche Bürgerforum im März 2014 in Kiel durchgeführt. Die Veranstaltungsorganisation ist in Kapitel 3 (Arbeitsverfahren – das Bürgerforum in Deutschland) unter Einbeziehung der organisatorischen Rahmenbedingungen, der Struktur der Teilnehmergruppe und Bewertung der Veranstaltung durch die Bürger im Detail beschrieben.

Das Kapitel 4 präsentiert die empirischen Forschungsergebnisse des Bürgerforums. Es stellt zuerst die allgemeine Einstellung der Bürger zu Privatsphäre und Sicherheit dar, gefolgt von mehr technologiespezifischen Meinungen der Veranstaltungsteilnehmer. Insgesamt nahmen die teilnehmenden Bürger eine recht kritische Haltung gegenüber Sicherheitstechnologien ein. Sie äußerten starke Bedenken hinsichtlich der Nutzung überwachungsfokussierter Technologien für Zwecke der inneren Sicherheit. Der Hauptgrund für diese Bedenken wurde darin gesehen, dass solche Technologien generell als die Privatsphäre sowohl auf persönlicher Ebene wie auch im Allgemeinen beeinträchtigend wahrgenommen werden. Hierbei wurde deutlich, dass die Bürger starke Zweifel an der Wirksamkeit von Überwachungstechnologien hinsichtlich erstrebter Verbesserung der inneren Sicherheit haben. Die Teilnehmer kritisierten das Fehlen verlässlicher und objektiver Evaluation des Einsatzes von Sicherheitstechnologien und sagten, dass sie sich nicht automatisch sicherer fühlten, sobald diese verwendet würden. Hinsichtlich überwachungsbasierter Sicherheitstechnologien im Allgemeinen sagten die Bürger, dass sie sich diesen Überwachungswerkzeugen ausgeliefert fühlen und kritisierten zugleich die Streubreite solcher breit überwachungsfokussierten Maßnahmen. Die Bürger denken, dass viele Sicherheitstechnologien unter Umständen sensible, sogar intime Informationen über unschuldige Personen in weitem Umfang offenbaren können. Während des gesamten Veranstaltungstages äußerten die Teilnehmer große Besorgnis über die aus ihrer Wahrnehmung immer stärker werdende Überwachung in allen Bereichen des Lebens und beklagten die schleichende Entwicklung der modernen Gesellschaft hin zu einem Panoptikon Setting. Viele Bürger gaben zu, dass sie einen Abschreckungseffekt auf ihr eigenes Verhalten (entsprechend dem Englischen Sprachbegriff "chilling effect") spürten, sobald sie sich bewusst würden, überwacht zu sein. Dennoch zeigten die Teilnehmer des Bürgerforums an diesem Tag ein sehr vielschichtiges Meinungsbild, wobei sie anerkannten, dass Sicherheitstechnologien prinzipiell neutrale Werkzeuge sind, die in Belangen der Sicherheit Vorteile bringen können. Jedoch nehmen die

Bürger diese Technologien als anfällig für Missbrauch durch Sicherheitsbehörden und unbefugte Dritte wahr.

Als Konsequenz dieser Risikowahrnehmung bemerkte eine recht große Anzahl von Teilnehmern, dass sie sich aktiv Sicherheitstechnologien widersetzen würden, da sie sich durch das Gefühl des Überwachtseins allgemein sehr unbehaglich fühlten. Zudem gaben Bürger in den Gruppendiskussionen an, sich nicht nur durch staatliche Überwachung unsicher zu fühlen, sondern zusätzlich auch durch die weitverbreitete Sammlung personenbezogener Daten durch Privatfirmen für kommerzielle Zwecke. Dies schien vor allem einen erheblichen Einfluss auf ältere Teilnehmer zu haben, welche sich durch die Komplexität moderner Technologien überfordert fühlten. Infolge dieser Unsicherheiten sagten einige Teilnehmer, dass sie die Nutzung solcher Technologien, wie etwa Mobiltelefone, Computer etc. vollständig vermeiden würden.

In Bezug auf gesellschaftliche oder individuelle Aspekte sagten die Teilnehmer ausdrücklich, dass die deutsche Regierung verpflichtet sei, sowohl die Privatsphäre und die demokratischen Freiheiten der deutschen Bürger zu schützen wie auch die öffentliche Sicherheit zu garantieren. Die Bürger beklagten, dass staatliche Einrichtungen aus ihrer Perspektive oftmals den Sicherheitszielen zu viel Priorität einräumten. Sie kritisierten, dass dies ein zu einseitiger Fokus sei, der mit einem starken Glauben an Technik als Lösung für Sicherheitsprobleme einherginge. Als Folge fühlten sich die Bürger ganz persönlich unbehaglich gegenüber staatlicher Überwachung. Jedoch sei dieses Gefühl nicht nur beschränkt auf lediglich persönliche Betroffenheit. Vielmehr riefen ebenfalls die breiteren gesellschaftlichen Auswirkungen des Einsatzes von Sicherheitstechnologien durch Regierungen Besorgnis hervor, insbesondere im Hinblick auf potentielle negative Effekte auf Menschenrechte und demokratische Prinzipien. Von Teilnehmern genannte Aspekte waren hierbei die Furcht vor Regierungen, welche ihre Bürger per se unter Generalverdacht stellen und vor daraus resultierender schleichender, Big-Brother-hafter Ausweitung von Überwachung für Sicherheitszwecke. In Bezug auf technologiespezifische Aspekte hoben die Bürger die inhärenten Missbrauchsrisiken hervor, die dazu führen könnten dass eine faktische Diskriminierung bestimmter Bevölkerungsgruppen, insbesondere Minderheiten, erfolgt. Zudem wurde der Missbrauch von Überwachungstechnologien für politische Zwecke mehrfach mit Verweisen auf den sogenannten Arabischen Frühling erwähnt. Die teilnehmenden Bürger bemerkten, dass, obgleich Deutschland eine demokratische Staatsform hat, dies für seine Bürger nicht automatisch immer der Fall sein mag. Aufgrund der historischen Erfahrungen der deutschen Bevölkerung mit repressiven Regimes betonten die Teilnehmer, dass dies ein ernstzunehmendes Risiko sei, wenn es um überwachungsbasierte Sicherheitstechnologien geht. Aber schon ohne einen direkten und gewollten Missbrauch von aus Überwachung gewonnener Information wurde herausgestellt, dass es ein immer größer werdendes Risiko der schleichenden Aushöhlung der verfassungsgemäß garantierten Unschuldsvermutung gebe. Schlussendlich kann gesagt werden, dass die auf dieser Veranstaltung geäußerten Meinungen der Bürger, dass die allmähliche Erosion der Privatsphäre auf beiden Ebenen, persönlich wie gesellschaftlich, ein tiefes Misstrauen gegenüber der staatlichen Nutzung von überwachungsbasierten Sicherheitstechnologien erzeugt und schürt.

Dieses Misstrauen in staatliche Sicherheitspolitik und entsprechende Aktivitäten wurde auch deutlich, als die Teilnehmer bei dem Bürgerforum die Chance hatten, ihre Meinung bezüglich der Vertrauenswürdigkeit von Sicherheitsbehörden im Allgemeinen kund zu tun. Eine solche Vertrauenswürdigkeit unter der Annahme von Wohlwollen und Kompetenz staatlicher Sicherheitseinrichtungen wurde von der Mehrheit der Bürger der Veranstaltung angezweifelt. Unter Bezugnahme auf die besprochenen Sicherheitstechnologien war hierbei das Vertrauen ein wenig größer in die staatliche Nutzung intelligenter Videoüberwachung im Vergleich zur Nutzung von Handyortung. Jedoch waren die Prozentergebnisse bezogen auf die Vertrauenswürdigkeit in Verbindung mit der Nutzung von Sicherheitstechnologien ganz generell nicht sonderlich hoch. Wiederholt betonten die Teilnehmer die Eingriffsintensität von Sicherheitstechnologien und deren Missbrauchsrisiko und argumentierten während der Gruppendiskussionen, dass das geringe Maß an Vertrauen in einem stark wahrgenommenen Mangel an Transparenz von staatlicher Seite begründet liege. Diese unzureichende Transparenz führe zu Unsicherheit hinsichtlich der rechtlichen und faktischen Rahmenbedingungen für den Einsatz von Sicherheitstechnologien und deren Zwecke. Die Erwähnung der NSA-Enthüllungen und des Arabischen Frühlings legen nahe, dass die Bürger diese Unsicherheit noch stärker fühlen, sobald ausländische Sicherheitsinstitutionen involviert sind.

Infolgedessen sagte die Mehrheit der Bürger, dass sie einen Paradigmenwechsel fort von technologieabhängigen Sicherheitslösungen hin zu einem Mehr an "Faktor Mensch" unterstützen würde, welches Raum lässt für alternative Ansätze, denen ihrer Meinung nach höhere Priorität eingeräumt werden sollte. In Bezug auf dennoch notwendige technische Sicherheitslösungen verlangten die Teilnehmer klarere und einheitlichere rechtliche Rahmenbedingungen mit effektiven Mitteln der Durchsetzung.

Zum Ende des Bürgerforums hin hatten die Teilnehmer die Gelegenheit, Empfehlungen an politische Entscheidungsträger für den Sicherheitsbereich auf europäischer wie auf nationaler Ebene zu formulieren. Mit diesen Empfehlungen erkennen die Teilnehmer im Prinzip an, dass unter bestimmten Umständen der Einsatz von überwachungsbasierten Sicherheitstechnologien gerechtfertigt sein kann, um Straftaten aufzuklären oder zu verhindern. Dennoch reflektieren die Empfehlungen die eingangs beschriebenen Bedenken der Bürger hinsichtlich der Streubreite aktuell eingesetzter wie auch vorhersehbar geplanter Maßnahmen verbunden mit großflächiger Datensammlung und negativen Folgen für die Privatsphäre und anderen Grundrechten. Hierbei nahmen die Teilnehmer die Chance wahr, konkrete Vorschläge in diesen Empfehlungen zu formulieren. Diese umfassen eine große Bandreite von Möglichkeiten, wie die oben beschriebenen wesentlichen Bedenken ihrer Meinung nach adressiert werden könnten. Diese Vorschläge beinhalten zusammengefasst:

- Erhöhte Transparenz bezüglich der Nutzung von Sicherheitstechnologien, ihrer Zwecke und Behandlung der erhobenen Daten,
- angemessene und aussagekräftige Evaluation überwachungsbasierter Sicherheitstechnologien auf der Basis objektiver Forschung,
- Aufsicht und Kontrolle dieser Technologien einsetzenden Sicherheitsbehörden
- Privacy by Design für spezifische Sicherheitstechnologien soweit möglich, um Missbrauchsrisiken zu reduzieren,
- Transparenz, Aufsicht und Kontrolle sollen realisiert werden mittels geeigneten, notwendigen, und wirksamen Maßnahmen auf organisatorischer, technischer, und rechtlicher Ebene.

Insbesondere was ausländische Sicherheitseinrichtungen betrifft, enthalten die Empfehlungen eine Forderung nach einem einheitlichen und internationalen rechtlichen Regelwerk zumindest auf europäischer Ebene, das auch einfach für den europäischen Bürger durchsetzbar bzw. einklagbar ist. Die Texte der Empfehlungen machen deutlich, dass dies nicht nur für die staatliche Nutzung von Technologien gelten soll, sondern auch für den Privatsektor, um einen besseren Schutz der Privatsphäre zu gewährleisten und zugleich die Bürgerrechte generell zu stärken. Die Bürger unterstützen schon die Idee von weniger Überwachung im Allgemeinen, mit einem stärkeren Fokus auf alternative Ansätze. Genannte Beispiele für solche alternativen Ansätze sind:

- Investition in mehr Polizeipersonal,
- politische und faktische Lösungen zur Armutsbekämpfung und andere Arten sozialer Ungleichheit,
- nicht technische Kriminalprävention, wie etwa Sozialprogramme,
- mehr Bildung,
- Erforschung weiterer Möglichkeiten zur Adressierung von Sicherheitsproblemen.

Schlussendlich kann gesagt werden, dass obgleich dass eine große Gruppe sehr kritischer Bürger an dem Bürgerforum teilgenommen haben, diese dennoch merklich bemüht waren, eine vielschichtige Betrachtung der diskutierten Themen vorzunehmen. Hierbei wurden Argumente pro und contra unter Einbeziehung der Tatsache, dass ein freier und demokratischer Staat auch erfordert, seinen Bürgern ein angemessenes Maß an Sicherheit zu garantieren, sorgfältig untersucht. Indes, die wahrgenommenen negativen Effekte von Überwachung auf persönlicher wie auch auf gesellschaftlicher Ebene besorgen deutsche Bürger sehr. Aus diesem Grund kann gesagt werden, dass das oft zitierte Trade-Off Modell die Probleme zu stark vereinfacht, da Überwachung zu Sicherheitszwecken auch eine Ursache für Unsicherheit aus Bürgersicht sein kann. Darüber hinaus wird dieses Modell den komplexen Realitäten rund um Fragestellungen der

Sicherheitspolitik und Praxis nicht gerecht. Folgerichtig muss eher eine ausgewogenere Balance zwischen Privatsphäre und Sicherheit angestrebt werden, ohne eine der beiden Aspekte zu stark zu vernachlässigen. Diese Konsequenz korreliert mit den auf dem Bürgerforum geteilten Meinungen der Teilnehmer und deren Erwartung, dass deutsche wie europäische Entscheidungsträger im Hinblick auf die Erreichung einer solchen Balance aktiv werden. Nach Auffassung der Bürger sind solche Bemühungen unerlässlich, um die Errungenschaften der modernen europäischen Gesellschaft im Hinblick auf demokratische Freiheiten und Grundrechte europäischer Bürger zu wahren.

1 Einleitung

Dieses Dokument fasst das Ergebnis des deutschen Bürgerforums zusammen, das im Rahmen des von der Europäischen Union geförderten Projekts SurPRISE im März 2014 in Kiel durchgeführt wurde.

Dieses Bürgerforum hatte zum Ziel, die Meinungen von deutschen Bürgern im Hinblick auf Privatsphäre und Sicherheit zu ermitteln. Dazu wurden unter anderem zwei spezifische beispielhafte überwachungsbasierte Sicherheitstechnologien (Intelligente Videoüberwachung und Handyortung) behandelt. Es wurden in insgesamt neun verschiedenen Ländern Bürgerforen mit durchschnittlich je 200 Teilnehmern durchgeführt. Hierbei folgte die gesamte Durchführung aller einzelnen Veranstaltungen einem vordefinierten und einheitlichen Ablauf, um die Vergleichbarkeit der Ergebnisse zu gewährleisten. Die Ergebnisse wurden in neun verschiedenen Länderreports jeweils pro Land präsentiert, und in einem Gesamtreport länderübergreifend und vergleichend zusammengefasst.

Die Analyse enthält sowohl qualitative wie auch quantitative Elemente auf der Basis der von den Teilnehmern beim Bürgerforum geäußerten Meinungen. Das Ziel der Analyse ist es, einen Überblick über die Sichtweise der Bürger auf die behandelten Themen zu geben, damit diese bei zukünftigen Gesetzen und Richtlinien berücksichtigt werden können.

2 Durchführung des Bürgerforums in Deutschland

2.1 Ablauf der Veranstaltung

Vor dem Veranstaltungstag des Bürgerforums wurden den Teilnehmern eine Informationsbroschüre und organisatorischen Hinweisen zugeschickt. Die Infobroschüre enthielt eine erste thematische Einführung in die Sicherheitstechnologien, die Inhalt des Bürgerforums waren. Im Mittelpunkt standen zwei beispielhafte Sicherheitstechnologien, die dazu dienten die Meinung der Bürger in Bezug auf Privatsphäre und Sicherheit zu ermitteln.

Zu dem Bürgerforum wurden insgesamt 221 Bürger als Teilnehmer eingeladen. Es sind insgesamt 190 Teilnehmer am Veranstaltungstag erschienen. Bei dem Auswahlprozess konnten leider nicht alle Anmeldungen berücksichtigt werden. Das Bürgerforum dauerte ca. 7 Stunden und wurde an einem Samstag durchgeführt. Die Teilnehmer wurden in dem Veranstaltungsraum in Gruppen an einzelnen Tischen platziert. Die Einführung der Teilnehmer in die Thematik des Bürgerforums wurde durch mehrere Kurzfilme unterstützt, die im Laufe des Veranstaltungstages vorgeführt worden. Der Veranstaltungstag enthielt ebenfalls Gruppendiskussionen und Befragungen der Teilnehmer. Die Befragung der Teilnehmer wurde mittels eines elektronischen Abstimmungssystems durchgeführt. Alle Teilnehmer hatte somit die Möglichkeit gleichzeitig die Abstimmungsfragen zu beantworten. Die Ausarbeitung und Diskussion von Politikempfehlungen rundeten die Veranstaltung ab. Zusätzlich hatten die Teilnehmer die Möglichkeit, Aspekte, die ihrer Ansicht nach im Rahmen des Bürgerforums nicht ausreichend berücksichtig werden konnten in Form von Postkarten an die Politik zu äußern. Die Meinungsäußerungen sind ebenfalls in die Auswertung eingeflossen.

2.2 Struktur der Teilnehmergruppe

Dieser Abschnitt beschreibt die demografische Struktur der Teilnehmergruppe vom Bürgerforum in Kiel. Die Ergebnisse zu den Einzelfragen werden der Übersichtlichkeit halber zusätzlich tabellarisch dargestellt. Die einzelnen Fragen sind hierbei stets mit dem Kürzel Q plus Fragennummer bezeichnet (also z. B. Q2, Q3 etc.), um eine bessere Zuordnung zu dem vollständigen Fragenset, welches im Projekt entwickelt wurde, zu ermöglichen. Insgesamt wurden 221 Bürger zu dem Bürgerforum eingeladen, von denen 190 am Veranstaltungstag erschienen und teilnahmen. Von den Teilnehmern, die die Frage nach dem Alter beantwortet haben (wird im Folgenden jeweils mit N benannt) gab die Mehrheit von 28,2 % an aus der Altersgruppe der 40–49-Jährigen zu stammen. Die kleinste Altersgruppe stellten die über 70-Jährigen mit nur 1,6 % der Gesamtzahl (siehe Tabelle unten).

Q01 - Alter (Gesamtheit gültiger Antworten: N= 188)

18-29 Jahre alt	23,4 %
30-39 Jahre alt	11,7 %
40-49 Jahre alt	28,2 %
50-59 Jahre alt	23,9 %
60-69 Jahre alt	11,2 %
über 70 Jahre alt	1,6 %

Tabelle 1: Überblick über die verschiedenen Altersgruppen

Von der Gesamtzahl der votierenden Teilnehmer gaben 35,8 % ihr Geschlecht mit weiblich an während die 62,6 % ihr Geschlecht mit männlich angaben. 1,6 % machten keine Angabe zu ihrem Geschlecht. Die Verteilung von Alter und Geschlecht wird in Abbildung 1 dargestellt.

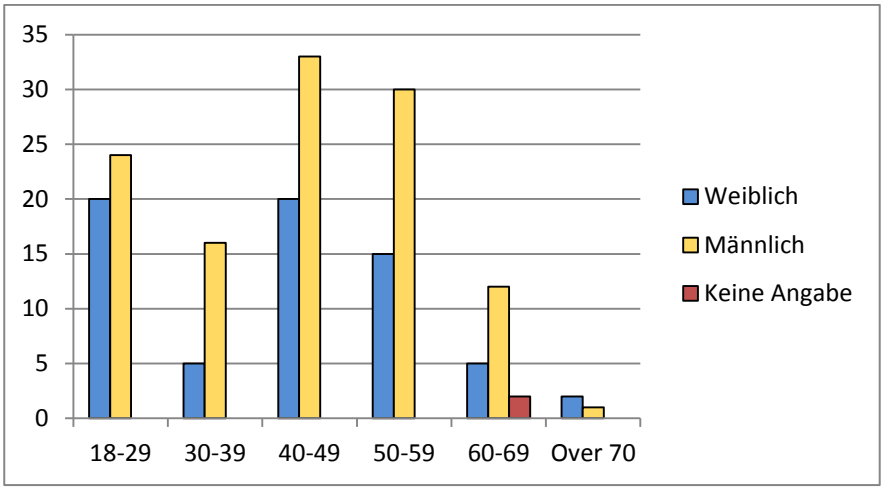

Abbildung 1: Geschlechts- und Altersverhältnis der Teilnehmer

Ferner haben 17,0 % der teilnehmenden Bürger in ihrem Haushalt Kinder im Alter von 16 Jahren oder jünger, während 78,6 % angaben, kinderlos zu sein und 4,4 % keine Angabe machten.

Die Mehrzahl der Teilnehmer sagte, dass sie aus einem städtischen Gebiet kämen (64,8 %) und 28,6 % gaben an, aus einem eher ländlichen Bereich zu kommen. Dieses Ergebnis spiegelt im Wesentlichen die Demografie von Kiel als mittelgroßer Stadt und seiner recht großen ländlichen Umgebung wieder. Etwa 5,5 % der Teilnehmer gab an, aus einem großstädtischen Gebiet zu kommen.

Die Ergebnisse der Fragen zeigen dass der Ausbildungsgrad der Teilnehmergruppe insgesamt betrachtet recht hoch ist. Eine große Mehrheit von 27,9 % sagte, dass sie einen Universitätsabschluss oder Vergleichbares hätten, 36,6 % gaben an, einen Fachhochschul- oder Grundstudiumsabschluss zu haben oder eine fachliche Berufsausbildung mit Abschluss (siehe Tabelle unten).

Q100 – Höchster Grad der Ausbildung (N= 183)

Grundschule	1,6 %
Hauptschulabschluss, Realschulabschluss oder vergleichbar	12,0 %
Fachhochschulreife, Hochschulreife (Abitur) oder vergleichbar	18,6 %
Fachliche Berufsausbildung mit Abschluss	16,4 %
Fachhochschul- oder Grundstudiumabschluss oder vergleichbar	20,2 %
Universitätsabschluss oder vergleichbar	27,9 %
Keine Angabe	3,3 %

Tabelle 2: Höchster Grad der Ausbildung

Die meisten Bürger sagten, dass sie in einem Beschäftigungsverhältnis stünden (42,9 %). Darüber hinaus wies die Teilnehmergruppe eine beachtliche Anzahl von Studenten (17,6 %) und Selbstständigen (13,2 %) auf.

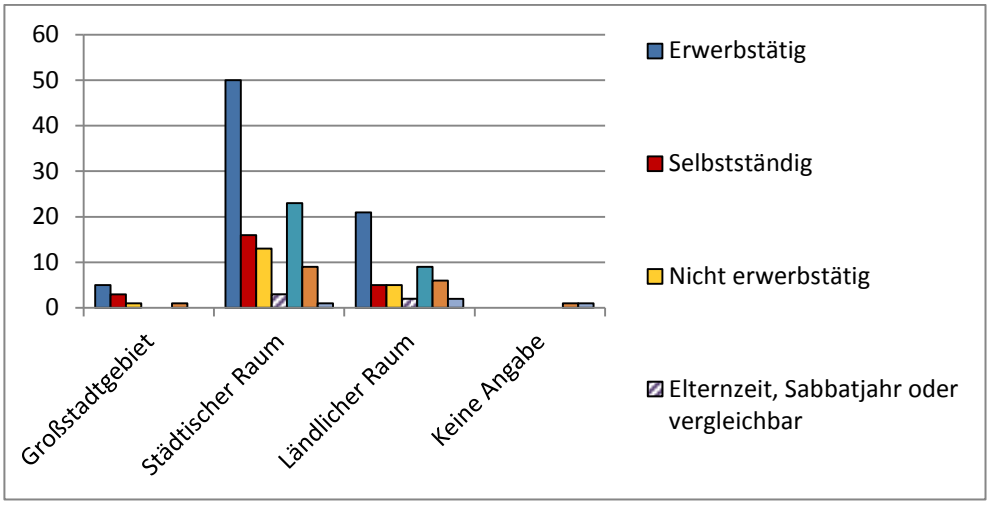

Abbildung 2: Beschäftigungsverhältnis der Teilnehmerinnen und Teilnehmer per Wohnbereich

Von den Teilnehmern, die die folgende Frage beantwortet haben (N = 181) gab die Mehrzahl (30,4 %) an, eine spezifische Berufsausbildung (Experte) abgeschlossen zu haben. Die zweitgrößte Anzahl der antwortenden Teilnehmer (21,0 %) sagte, sie sei in leitender Funktion tätig (Manager, leitende(r) Angestellte(r) oder Staatsbedienstete(r) mit Leitungsfunktion) während nur eine kleine Zahl angab, im Bereich Produktion und Bauwesen tätig zu sein (1,7 %).

Das Einkommen (verglichen mit dem bundesdeutschen Durchschnitt) war von der Mehrzahl der Teilnehmer als unter dem Durchschnitt bewertet worden (43,0 % sagten, sie verdienten weniger oder sogar erheblich weniger). Dagegen sagten 33,5 %, dass sie mehr oder erheblich mehr als der Durchschnitt verdienen würden. Eine recht große Zahl von 17,9 % aller Antwortenden wählte bei dieser Frage die Option "Keine Angabe".

Von der gesamten antwortenden Teilnehmergruppe bezeichnete sich die Mehrheit (91,1 %) als Bürger dieses Landes, während die übrigen Teilnehmer andere Staatsbürgerschaften angaben, hierbei 2,8 % mit doppelter Staatsbürgerschaft von zwei europäischen Ländern und 2,2 % mit doppelter Staatsbürgerschaft von nichteuropäischen Ländern. In diesem Zusammenhang wurden die Teilnehmer auch gefragt, ob sie sich einer Minderheit zugehörig fühlen würden. Die überwiegende Mehrheit (69,9 %) verneinte dies, während 19,7 % dies bejahten und eine Prozentzahl von 10,4 % die Antwortmöglichkeit "Keine Angabe" wählte.

Zusammenfassend kann festgestellt werden, dass die Teilnehmer eher mittleren Alters waren und mehr männliche als weibliche Personen anwesend waren. Generell war der Ausbildungsgrad recht hoch. Es kann vermutet werden, dass der größte Teil der Teilnehmer zur Gruppe der gebildeten Mittelschicht gehört. Aufgrund der thematischen Ausrichtung des Bürgerforums war dies zu erwarten. Bei der Rekrutierung der Teilnehmer des Bürgerforums wurde darauf Wert gelegt eine möglichst vielschichtige Zusammensetzung zu gewährleisten.

3 Empirische Ergebnisse des Bürgerforums

Im Folgenden werden die empirischen Ergebnisse des Bürgerforums in Kiel präsentiert. Die Ergebnisse wurden gewonnen aus den Antworten zu den Fragen an die Teilnehmer, aus den Notizen und Eindrücken der Tischmoderatoren und Protokollführer aus den Gruppendiskussionen, aus den Empfehlungen der Gruppen sowie den von einzelnen Teilnehmern abgegebenen Postkarten. In diesem Zusammenhang werden im Folgenden Tabellen und Abbildungen einen Überblick über die gewonnenen empirischen Ergebnisse liefern.

Das Hauptaugenmerk liegt bei der Auswertung der Ergebnisse darauf, die aus Sicht der Bürger entscheidenden Kriterien für die Akzeptanz und Akzeptierbarkeit von überwachungsbasierten Sicherheitstechnologien herauszufinden sowie Aufschluss über die wesentlichen Bedenken hinsichtlich der Privatsphäre zu gewinnen.

3.1 Allgemeine Einstellung zu Privatsphäre und Sicherheit

Bürgerforen wurden in neun verschiedenen Mitgliedstaaten der EU durchgeführt. Im Vergleich zeigte sich, dass die deutschen Teilnehmer eine deutlich kritischere Haltung in Bezug auf überwachungsbasierte Sicherheitstechnologien hatten als die Teilnehmer in den anderen Mitgliedstaaten. Im Allgemeinen schätzten die Teilnehmer ihre eigenen Kenntnisse hinsichtlich dieser Technologien bereits vor dem Bürgerforum als relativ fundiert oder zumindest durchschnittlich ein. Während 44,9 % sich selbst als sehr gut oder recht kenntnisreich benannten, gaben immer noch 36,0 % an, dass sie einiges über solche Technologien wissen (siehe Tabelle unten). Dies zeigt, dass die teilnehmenden Bürger offenbar bereits vor ihrer Teilnahme ein gewisses Bewusstsein hinsichtlich dieser Sicherheitstechnologien hatten.

Q6 – Wie würden Sie Ihren Wissenstand zu überwachungsbasierten Sicherheitstechnologien vor dem Lesen des SurPRISE-Informationsmaterials beurteilen? (N= 178)

Ich habe einen sehr guten Wissensstand darüber.	8,4 %
Ich weiß vieles darüber, würde aber gerne mehr wissen.	36,5 %
Ich weiß einiges darüber.	36,0 %
Ich weiß wenig bis nichts darüber.	18,0 %
Keine Angabe	1,1 %

Tabelle 3: Wissen über Überwachungstechnologien vor dem Bürgerforum

Am Ende des Veranstaltungstages wurden die Teilnehmer gebeten, ihren eigenen Kenntnisstand nach dem Lesen des Informationsmaterials, den Diskussionsrunden mit anderen Teilnehmern und den Kurzfilmen einzuschätzen. Als Antwort auf diese Frage gaben insgesamt 79,0 % an dass sie nunmehr entweder einen sehr guten oder einen recht guten Wissensstand hätten, während noch 17,7 % angaben, dass sie nach dem Bürgerforum einiges über Sicherheitstechnologien wüssten.

Q93 – Mit Broschüre und Filmen haben Sie einige Informationen erhalten und heute viel diskutiert. Wie würden Sie Ihr Wissen über überwachungsbasierte Sicherheitstechnologien nun beurteilen? (N= 181)

Ich habe einen sehr guten Wissensstand darüber.	22,1 %
Ich weiß vieles darüber, würde aber gerne mehr wissen.	56,9 %
Ich weiß einiges darüber.	17,7 %
Ich weiß wenig bis nichts darüber.	2,8 %
Keine Angabe	0,6 %

Tabelle 4: Wissen über Überwachungstechnologien nach dem Bürgerforum

Daraus wird - obgleich sich die Bürger bereits vor dem Bürgerforum als recht kenntnisreich einschätzen - deutlich erkennbar, dass sich der Wissensstand in Bezug auf Sicherheitstechnologien durch die Vorbereitung auf und die Teilnahme an der Veranstaltung erhöht hat.

Es wurden darüber hinaus Fragen zum eigenen Sicherheitsempfinden wie auch zur Einstellung gegenüber sicherheitsbasierten Überwachungstechnologien im Hinblick auf deren Nutzen für die Sicherheit und deren Risiken für die Privatsphäre gestellt.

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Ich fühle mich grundsätzlich sicher in meinem alltäglichen Leben.	Q3	188	21,3 %	45,2 %	29,3 %	3,7 %	0,5 %	0,0 %
Ich mache mir Sorgen über Sicherheit, wenn ich online bin.	Q4	187	31,6 %	25,1 %	26,7 %	12,8 %	3,2 %	0,5 %
Ich habe das Gefühl, dass man in diesem Land sicher leben kann.	Q5	186	26,3 %	47,3 %	21,5 %	1,6 %	2,7 %	0,5 %
Insgesamt bin ich der Ansicht, dass überwachungsbasierte Sicherheitstechnologien routinemäßig eingesetzt werden sollen, um die öffentliche Sicherheit zu verbessern.	Q7	181	9,4 %	14,4 %	23,8 %	21,0 %	30,9 %	0,6 %
Ich fürchte, dass der Einsatz von überwachungsbasierten Sicherheitstechnologien die Privatsphäre im Allgemeinen aushöhlt.	Q8	188	47,9 %	25,0 %	19,1 %	5,9 %	1,6 %	0,5 %
Ich befürchte, dass der Einsatz von überwachungsbasierten Sicherheitstechnologien meine Privatsphäre aushöhlt.	Q9	186	42,5 %	25,3 %	17,2 %	11,3 %	3,2 %	0,5 %
Alternativen Sicherheitskonzepten, die ohne technologische Mittel der Überwachung auskommen, sollte mehr Beachtung geschenkt werden.	Q10	186	47,8 %	23,1 %	19,9 %	4,8 %	2,2 %	2,2 %

Tabelle 5: Allgemeine Einstellung zu Sicherheit

Die Ergebnisse zeigen, dass sich die meisten Teilnehmer grundsätzlich relativ sicher in ihrem alltäglichen Leben fühlen. Ein größerer Prozentsatz der Antwortenden ist jedoch hinsichtlich der Sicherheit besorgt, wenn sie online aktiv sind. Hierfür kann es unterschiedliche Erklärungsansätze geben. Denkbar ist, dass einige Teilnehmer bereits schlechte Erfahrungen mit der Sicherheit im Internet hatten, wie zum Beispiel mit Malware, Identitätsdiebstahl oder ähnlichen Vorfällen. Vertiefend hinsichtlich der allgemeinen Haltung der Teilnehmer zu Privatsphäre und Sicherheit wurden erhebliche Bedenken hinsichtlich des Einsatzes überwachungsbasierter Sicherheitstechnologien zu Zwecken der öffentlichen Sicherheit deutlich (bei Q7 etwa 51,9 % insgesamt im Spektrum "Trifft eher nicht zu/Trifft überhaupt nicht zu"). Diese kritische Haltung verstärkte sich im Verlauf der Veranstaltung, sodass am Ende des Tages 60,1 % der Aussage, dass solche Technologien routinemäßig zu Zwecken der Sicherheit eingesetzt werden sollen, „eher nicht“ oder „überhaupt nicht“ zustimmten (siehe im Detail die Ergebnisse zu Q94 in Tabelle Nr. 14 in Kapitel 3.2.3). Darüber hinaus wurden Sicherheitstechnologien generell, wie auch auf persönlicher Ebene, als ein Risiko für die Privatsphäre wahrgenommen, während die

Unterschiede bei den Ergebnissen der Fragen Q8 und Q9 nahelegen, dass die wahrgenommenen gesellschaftlichen Auswirkungen eine leicht stärkere Bedeutung haben als die persönliche Betroffenheit. Dieser Eindruck wird bestätigt durch die Antworten zu den entsprechenden Fragen Q95 und Q96, die am Ende der Veranstaltung abgegeben wurden und sich darauf beziehen, inwieweit die Bürger hinsichtlich einer Erosion der Privatsphäre durch Sicherheitstechnologien generell und für sich persönlich besorgt sind (vgl. Tabelle Nr. 14 in Kapitel 3.2.3). Die Ergebnisse zu diesen späteren Fragen machen offenkundig, dass sich das Bewusstsein der Teilnehmer über die Gefährdung der Privatsphäre sowohl auf persönlicher, aber noch mehr auf gesellschaftlicher Ebene verstärkt hat.

3.2 Wie nehmen die Teilnehmer die Nutzung von Sicherheitstechnologien wahr?

Im Kontrast zur vorangegangenen Untersuchung der allgemeinen Haltung der Teilnehmer zu Sicherheitstechnologien und Privatsphäre wird sich der folgende Abschnitt auf wesentliche Aspekte der Akzeptanz und Akzeptierbarkeit von spezifischen Sicherheitstechnologien konzentrieren.

Zusätzlich wird der Grad der wahrgenommenen Erhöhung der Sicherheit mit Bezug zu den Auswirkungen und der Verhältnismäßigkeit des Technologieeinsatzes untersucht. Hierbei werden einerseits die wahrgenommene Wirksamkeit dieser Sicherheitsmaßnahmen und andererseits die wahrgenommene Beeinträchtigung durch diese berücksichtigt. Zudem werden die zentralen Bedenken der Teilnehmer im Hinblick auf Privatsphäre wie auch deren Haltung hinsichtlich Vermeidung oder gar Widerstand gegen Überwachung evaluiert. Dies beinhaltet sowohl die individuelle Sichtweise, wie auch kollektive Aspekte im Kontext persönlicher Erfahrungen verglichen mit der Bürgersicht auf allgemeine gesellschaftliche Werte.

Um die tiefergehenden Fragen in Verbindung mit den für das deutsche Bürgerforum spezifischen ausgewählten Sicherheitstechnologien vorzubereiten, wurden einleitende Fragen zum Bewusstsein und zum allgemeinen Wissen über die jeweilige Technologie gestellt. So zielte bei der intelligenten Videoüberwachung die Frage Q11 darauf ab, zu erfahren, ob und wie oft sich Bürger einer Kameraüberwachung in ihrem eigenen Wohn- und Lebensraum bewusst sind (siehe Tabelle unten). Die Ergebnisse zeigen, dass eine Mehrheit von 58,0 % angab, nie oder selten in der Gegend, in der sie wohnen, Überwachungskameras zu sehen, während 20,2 % antworteten, dass sie diese nur manchmal sehen würden. Ein noch immer recht großer Prozentsatz von 20,2 % gab jedoch an, sich optischer Kameraüberwachung im eigenen Wohn- und Lebensraum bewusst zu sein (häufig oder gar ständig).

Intelligente Videoüberwachung

			Nie	Selten	Manchmal	Häufig	Ständig	Keine Angabe
		N	**Prozentwerte**					
Wie häufig sehen Sie in der Gegend, in der Sie wohnen, Überwachungskameras?	Q11	188	23,4 %	34,6 %	20,2 %	12,2 %	8,0 %	1,6 %

Tabelle 6: Bewusstsein von Videoüberwachung

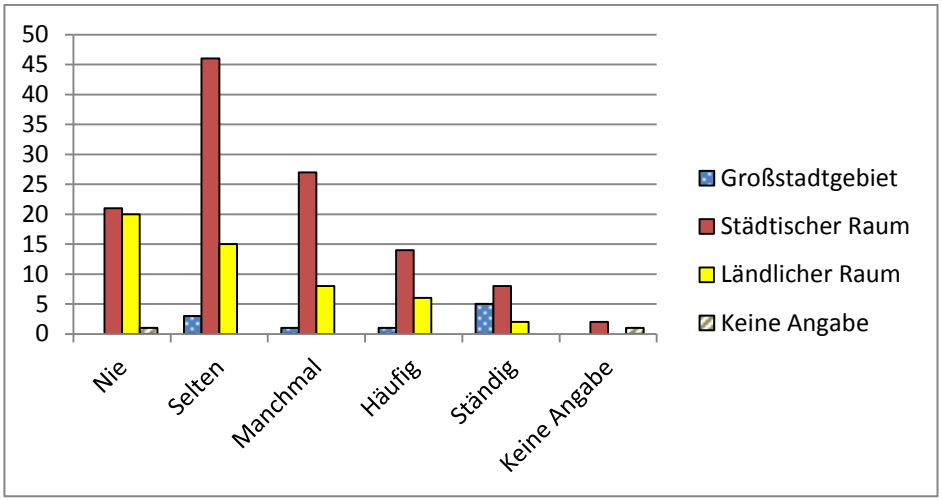

Abbildung 3: Bewusstsein von Videoüberwachung in grafisch visualisierter Form (Q11)

Folglich scheint es, als ob die Videoüberwachung öffentlichen Raumes im Allgemeinen eine eher unauffällige Maßnahme ist.

Die Antworten auf die Frage Q14 zeigen, dass die Mehrheit der Teilnehmer (82,2 %) auf der Grundlage des Informationsmaterials und den erklärenden Kurzfilmen sehr gut verstanden zu haben scheint, was intelligente Videoüberwachung eigentlich ist.

Intelligente Videoüberwachung

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Ich verstehe, was intelligente Videoüberwachung ist.	Q14	185	46,5 %	35,7 %	11,9 %	4,3 %	1,1 %	0,5 %

Tabelle 7: Technisches Verstehen der intelligenten Videoüberwachung

Die entsprechenden Fragestellungen hinsichtlich der Häufigkeit der Nutzung von Handys bzw. Smartphones und dem Verständnis dieser Technik finden sich in Q13 und Q16 (siehe Tabellen 8 und 9 unten). Q13 zeigt, dass die Mehrzahl der Teilnehmer (insgesamt 68,6 %) entweder häufig oder ständig Mobilgeräte wie Handys oder Smartphones nutzen, wohingegen 19,1 % angaben, solche Geräte nur manchmal zu nutzen und wenige Teilnehmer antworteten, diese nur selten (8,5 %) oder gar nie (3,7 %) zu benutzen.

Handyortung

			Nie	Selten	Manchmal	Häufig	Ständig	Keine Angabe
		N	**Prozentwerte**					
Wie häufig nutzen Sie mobile Geräte, wie z. B. Mobiltelefone oder Smartphones?	Q13	188	3.,7 %	8,5 %	19,1 %	16,5 %	52,1 %	0,0 %

Tabelle 8: Häufigkeit der Nutzung mobiler Geräte

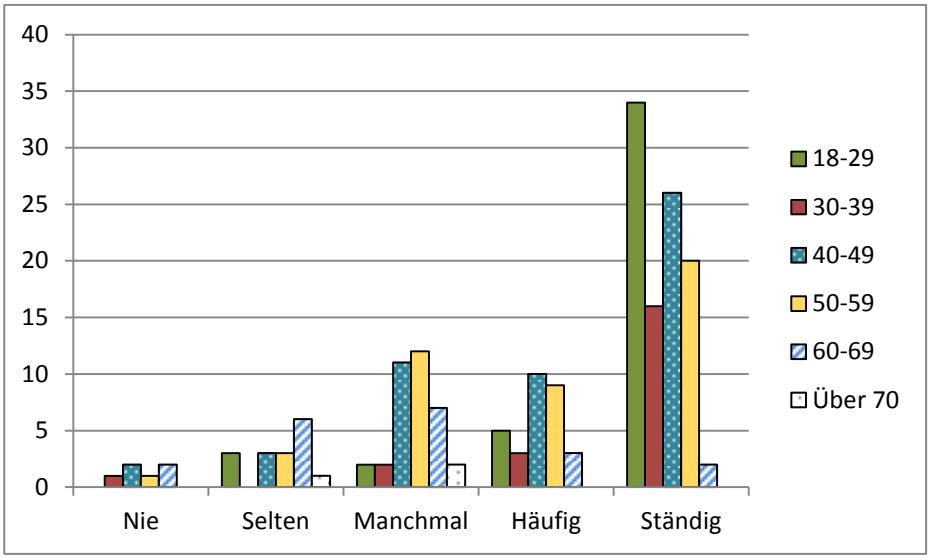

Abbildung 4: Häufigkeit der Nutzung mobiler Geräte in grafisch visualisierter Form (Q13)

Im Vergleich zur intelligenten Videoüberwachung schätzten die Bürger ihr eigenes Verständnis der jeweiligen Technik bei der Handyortung als erheblich höher ein, wie aus den Antworten zu Q16 ersichtlich wird.

Handyortung

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Ich verstehe, was Handy- bzw. Smartphone-Ortung ist.	Q16	186	74,2 %	18,3 %	4,8 %	1,1 %	1,1 %	0,5 %

Tabelle 9: Technisches Verstehen der Handyortung

So erscheint die Nutzung von Mobilgeräten durch deutsche Bürger relativ verbreitet, indem sie diese oftmalig oder gar regelmäßig im Alltag benutzen.

Insgesamt wird deutlich, dass, während intelligente Videoüberwachung und Handyortung zumindest teilweise neue Entwicklungen im Technikbereich darstellen, im Prinzip ein generelles Grundverständnis dieser Sicherheitstechnologien in recht kurzer Zeit von Bürgern entwickelt werden kann, sofern es in klarer und präziser Weise vermittelt wird. Daher erlangten die Teilnehmer durch das Informationsmaterial und die Kurzfilme eine grundlegende Basis für ihre folgende Einschätzung des Technologieeinsatzes und deren Auswirkungen während des Bürgerforums. Dies ermöglichte ihnen, ihre eigene Meinung zu diesen Technologien auszudrücken. Den Teilnehmern wurde hierbei jedoch auch bewusst gemacht, dass es nicht zentral darum geht, die technische Funktionsweise zu bewerten, sondern, dass vielmehr ihre Meinung zu den durch diese Technologien hervorgerufenen Beeinträchtigungen der Privatsphäre und zu den entsprechenden Akzeptanzfaktoren gefragt ist.

3.2.1 Wahrgenommene Wirksamkeit vs. wahrgenommene Beeinträchtigung durch Sicherheitstechnologien

Bei dem Bürgerforum hatten die Teilnehmer Gelegenheit, ihre Meinung zur Wirksamkeit der angesprochenen überwachungsbasierten Sicherheitstechnologien zu äußern. Zudem konnten sie ihre Gedanken zu den Beeinträchtigungen der Privatsphäre von Bürgern durch diese Technologien mitteilen. Hierbei adressierten die ersten einleitenden Fragen die allgemeine Haltung zur Nutzung dieser Technologien als Mittel zur Erhöhung der Sicherheit. Um einen

besseren Überblick über die Ergebnisse zu liefern, werden die folgenden Tabellen die Ergebnisse für jede Technologie detailliert aufschlüsseln.

Intelligente Videoüberwachung ("Smart CCTV")

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Meiner Meinung nach ist Smart CCTV ein wirksames Mittel für die öffentliche Sicherheit.	Q17	186	7,0 %	16,7 %	29,0 %	24,2 %	21,5 %	1,6 %
Smart CCTV bereitet mir Unbehagen.	Q18	187	43,9 %	27,3 %	10,7 %	11,2 %	6,4 %	0,5 %
Ich fühle mich sicherer, wenn Smart CCTV verwendet wird.	Q19	185	3,8 %	10,3 %	17,8 %	22,7 %	44,3 %	1,1 %
Ich habe den Eindruck, dass mir Smart CCTV ohne meine Einwilligung aufgezwungen wird.	Q20	182	67,0 %	15,4 %	6,0 %	2,7 %	6,0 %	2,7 %
Smart CCTV ist ein angemessenes Mittel, um öffentliche Sicherheits-bedrohungen zu bewältigen.	Q21	185	6,5 %	7,6 %	21,6 %	29,7 %	33,0 %	1,6 %
Smart CCTV beunruhigt mich nicht, solange es nur auf Kriminelle abzielt.	Q32	186	4,8 %	4,3 %	8,1 %	12,9 %	61,3 %	8,6 %
Ich bin darüber besorgt, wie sich der Einsatz von Smart CCTV künftig weiterentwickeln könnte.	Q33	181	61,3 %	19,3 %	8,3 %	6,1 %	3,9 %	1,1 %
Smart CCTV beunruhigt mich nur, wenn es in Gebieten eingesetzt wird, wo ich lebe und arbeite.	Q34	182	3,8 %	4,4 %	4,4 %	13,2 %	68,7 %	5,5 %

Tabelle 10: Wahrgenommene Wirksamkeit intelligenter Videoüberwachung

Wie diese Ergebnisse zeigen, nehmen viele Bürger die intelligente Videoüberwachung nicht als ein wirksames Mittel für die Erhöhung der Sicherheit wahr (bei Q17: 45,7 % insgesamt im Spektrum "Trifft eher nicht zu" bis "Trifft überhaupt nicht zu"). Ein großer Prozentsatz von 29,0 % sah diese Frage differenziert („Teils, teils"), während nur 23,7 % sagten, dies träfe eher oder vollständig zu.

Hierbei gab eine große Mehrzahl der Teilnehmer an, sich durch intelligente Videoüberwachung unbehaglich zu fühlen (Q18). In diesem Kontext ist zu bemerken, dass ein hoher Prozentsatz von 43,9 % angab, dieses Statement träfe vollständig zu, während noch immer 27,3 % die einfache Zustimmung ("Trifft eher zu") als Antwortoption wählte, was insgesamt eine Rate von 71,2 % der Teilnehmer ergibt, die sich infolge von intelligenter Videoüberwachung im öffentlichen Raum unbehaglich fühlen. Konsistent mit diesem Statement stimmten lediglich 14,1 % der Teilnehmer der Aussage zu, sich durch die Observation mittels intelligenter Videoüberwachung sicherer zu fühlen (Q19), während im Gegenzug 67,0 % äußerten, dies träfe eher nicht oder überhaupt nicht zu. Vielmehr drückte eine große Zahl von Teilnehmern aus, den Eindruck zu haben, dass ihnen intelligente Videoüberwachung ohne deren Einwilligung aufgezwungen werde (82,4 % aus dem "Trifft eher zu" und "Trifft vollständig zu" Spektrum). Hierbei lehnten 62,7 % das Statement, dass diese Technologie ein angemessenes Mittel sei, um öffentliche Sicherheitsbedrohungen zu bewältigen, ab, während 21,6 % sich unentschlossen zeigten..

Dabei ist ein interessanter Aspekt, dass die Bürger ihre ablehnende Haltung hinsichtlich intelligenter Videoüberwachung als Mittel der Sicherheit nicht von ihrer persönlichen Betroffenheit abhängig machten. Dies wird durch die Ergebnisse der Frage Q32 deutlich, bei welcher 61,3 %

angaben, es träfe überhaupt nicht zu und noch 12,9 % sagten, es träfe eher nicht zu, dass sie nicht durch intelligente Videoüberwachung beunruhigt seien, soweit sie nur auf Kriminelle abzielt.

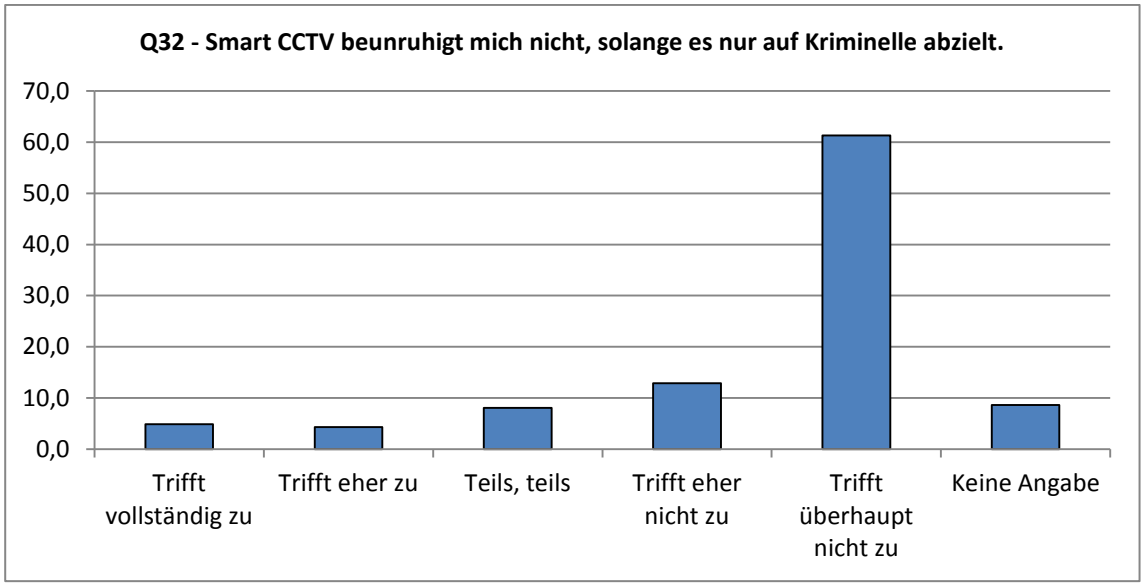

Abbildung 5: Bedeutung persönlicher Betroffenheit in Bezug auf intelligente Videoüberwachung

In Bezug auf die geäußerten Unsicherheiten oder Zweifel bezüglich der Wirksamkeit intelligenter Videoüberwachung als sicherheitserhöhende Maßnahme zeigen die Antworten zu Q33, dass mit einem Prozentsatz von 70,6 % die meisten der Teilnehmer über die mögliche zukünftige Entwicklung dieser Technologie besorgt sind. Eine Mehrheit sagte, dass es nicht zuträfe, nur dann durch intelligente Videoüberwachung beunruhigt zu sein, wenn diese in Gebieten eingesetzt würde, wo sie leben und arbeiten (Q34). Hierbei wählte eine Gesamtheit von 71,9 % entweder die Antwortoption "Trifft eher nicht zu" oder gar "Trifft überhaupt nicht zu".

Über die allgemeine Haltung der Bürger in Bezug auf die Nutzung der zwei angesprochenen Sicherheitstechnologien als Sicherheitsmaßnahmen adressierten die weiteren Fragen auch die wahrgenommene Beeinträchtigung durch diese, wobei auch hier weiter darauf eingegangen wurde, ob die Teilnehmer diese auch als nützlich ansehen (siehe Tabelle unten).

Q78 - Wählen Sie jene Aussage, die Ihrer Meinung am ehesten entspricht. (N= 184)

Smart CCTV ist sinnvoll und greift nicht besonders tief in die Privatsphäre ein.	8,7 %
Smart CCTV ist sinnvoll, greift aber tief in die Privatsphäre ein.	28,8 %
Smart CCTV ist nutzlos und greift tief in die Privatsphäre ein.	54,9 %
Smart CCTV ist weder sinnvoll noch greift es in die Privatsphäre ein.	1,1 %
Keine Angabe	6,5 %

Tabelle 11: Wahrgenommene Eingriffsintensität intelligenter Videoüberwachung

Hierbei sieht eine große Mehrheit der Teilnehmer (54,9 %,) die intelligente Videoüberwachung als nutzlos, aber tief in die Privatsphäre eingreifend an, während 28,8 % diese Technologie als nützlich, aber immer noch tief in die Privatsphäre eingreifend wahrnehmen. Nur 8,7 % stimmten dem Statement, intelligente Videoüberwachung sei nützlich und nicht in die Privatsphäre eingreifend, zu.

In der Gruppendiskussion rund um intelligente Videoüberwachung erkannten die Bürger an, dass die visuelle Überwachung des öffentlichen Raumes manche Vorteile haben kann. Zum Beispiel wurde angenommen, dass die Beobachtung von Kriminalitätsschwerpunkten eine abschreckende Wirkung auf mögliche Straftäter haben könnte und diese Maßnahme für kriminalpräventive Zwecke nützlich sein könnte. Zudem könnte die Detektion von gefährlichen Objekten durch die

hochentwickelten Funktionen intelligenter Kameras die Sicherung besonders gefährdeter Orte, wie etwa Flughäfen oder Bahnhöfe, unterstützen. Weiterhin sagten die Teilnehmer, dass eventuell auf diese Weise durch eine Verhinderung von Unglücksfällen die Sicherheit bei Großveranstaltungen erhöht werden könnte. Ein spezifisches Beispiel, das in diesem Zusammenhang genannt wurde, war die Massenpanik bei der Love Parade in Duisburg im Jahr 2010, bei der 21 Menschen getötet und mehrere hundert Menschen verletzt wurden. Neben der Prävention führten die Teilnehmer einen möglichen Nutzen zur Aufklärung von Straftaten an, indem die Kameraaufzeichnungen unter Umständen zu einer höheren Aufklärungsrate als anderes Beweismaterial, wie etwa Zeugenaussagen, führen könnten. Eine Bürgerin erzählte von ihrer Tochter, die für einige Zeit von einem Stalker verfolgt wurde. Bei diesen Vorfällen hätte sie sich zur Sicherheit ihres Kindes mehr Kameras im öffentlichen Raum gewünscht. Andere positive Aspekte rund um intelligente Videoüberwachung sind die mögliche Unterstützung des Sicherheitspersonals, die Reduzierung von Personalkosten und die Begrenzung menschlicher Willkür, da die Algorithmen neutralere Entscheidungsgrundlagen für sicherheitsrelevante Aktivitäten bieten könnten. Zusätzlich wurde angenommen, dass diese Technologie, obgleich noch sehr neu, innerhalb kurzer Zeit recht zuverlässig arbeiten und den unterschiedlichsten Zwecken dienen kann, wie etwa intelligentem Verkehrsmanagement inklusive Gefahrenwarnungen oder vereinfachten Verfahren zum Beispiel für Mautgebührenerhebungen oder Stadtplanung.

Die Bürger hatten jedoch auch erhebliche Kritik an intelligenter Videoüberwachung im Speziellen, wie auch Kameraüberwachung im Allgemeinen anzubringen. Während Kameraüberwachung im Privatsektor als durchaus nützlich zum Beispiel bei Ladendiebstahl (auch wenn die Beobachtung den Arbeitnehmerdatenschutz berührt) angesehen wurde, wurde angezweifelt, ob staatliche Videoüberwachung insgesamt wirksam gegen Kriminalität ist. Hierbei wurde angenommen, dass Straftäter und Terroristen eine solche Überwachung entweder umgehen oder solche technischen Systeme austricksen könnten. Andere angebrachte Bedenken waren, dass die Technologie teuer sei, Kriminalitätsschwerpunkte nur verlagert würden und Polizeipräsenz reduziert würde. Die Teilnehmer stellten Fragen dahingehend, welchen Schutz die Überwachungskameras Personen in konkreten Gefahrensituationen tatsächlich bieten können und merkten an, dass verstärkte Polizeipräsenz in gefährlichen Gebieten anstelle von mehr Videoüberwachung wirksamer sei. Weiterhin fürchten die Teilnehmer des Bürgerforums, dass eine spürbare Überwachung die Zivilcourage von Mitbürgern reduzieren könnte. Ein Grund hierfür könnte darin liegen, dass Bürger ein Gebiet infolge der Kameraüberwachung als sicherer wahrnehmen könnten oder im Falle eines Vorfalls annehmen, dass die visuelle Erfassung des Areals zu einer Alarmierung von Sicherheitspersonal führe. Daher wurde stark angezweifelt, dass intelligente Videoüberwachung die Empathie, Erfahrungen und Instinkte von Polizeibeamten im Streifendienst vollständig ersetzen könnte, und es wurde angemerkt, dass die Technologie niemals eine ultimative Entscheidungsbefugnis aufgrund ihrer "intelligenten" Algorithmen haben kann und sollte.

Die Hauptkritik hinsichtlich intelligenter Videoüberwachung war die Ablehnung allumfassender Überwachung von Bürgern im öffentlichen Raum, wobei die Frage, ob dies zu einem erhöhten Sicherheitsgefühl oder zum genauen Gegenteil führe, Gegenstand heftiger Debatten an manchen Tischen war. Das Gefühl eines „Panopticon Settings“ wurde hierbei erwähnt, und viele Teilnehmer sagten, dass sie, sobald sie sich einer Kameraüberwachung bewusst seien, anders verhalten würden, bis hin zu dem Punkt, von bestimmten Tätigkeiten abgeschreckt zu sein, wie etwa der Teilnahme an Demonstrationen. Ein zentraler Punkt der Kritik war dabei, dass die sogenannten "intelligenten" Aspekte dieser Technologie hauptsächlich einen Bezug zur Erkennung von Anomalien menschlichen Verhaltens haben. Die Bürger drückten Besorgnis darüber aus, wer definieren mag, welches Verhalten noch als "normal" angesehen werden soll und reflektierten hierbei über die Auswirkungen solcher Festlegungen auf die Gesellschaft. Abhängig davon, wie "abnormales" Verhalten definiert sein mag, sind die Teilnehmer sehr besorgt darüber, dass die Bevölkerung dadurch einer externen Vorbestimmung neuer moralischer Grundsätze ausgesetzt werden könnte. Die Bürger nehmen diese Technologie dahingehend wahr, dass sie atypisches Verhalten, welches zu Fehleinschätzungen führen könnte, in zunehmendem Maß weniger tolerieren könnte. Hierbei gibt es Sorge, dass auf diese Weise Unschuldige kriminalisiert werden, weil ihr Verhalten nicht der Norm entspricht, wie etwa Minderheiten, Kinder oder behinderte Menschen. Als Ergebnis hiervon nahmen die Teilnehmer an, dass die intelligente Videoüberwachung auch ein gewisses Diskriminierungspotential hat, da

sie Einzelne stigmatisieren könnte. Dies wurde explizit als ein mögliches Szenario genannt, soweit die gesammelten Kameraaufzeichnungen mit bereits existierenden Informationen aus unterschiedlichen Quellen, wie etwa Polizeidatenbanken, abgeglichen und verbunden werden. Ein genanntes Beispiel war jenes eines verurteilten Straftäters, der seine Strafe verbüßt habe, dessen Foto aber noch in polizeilichen Dateien gespeichert sei. Hierdurch bestehe die Möglichkeit, dass dieser zum Beispiel aufgrund Gesichtserkennung von Kameras dauerhaft stigmatisiert wird, was seine Resozialisierung und Wiedereingliederung in die Gesellschaft gefährden könnte. Insgesamt wurde eine flächendeckende Überwachung durch intelligente Kameras als ein Risiko für die verfassungsmäßig garantierte Unschuldsvermutung und als leichtes Ziel für Missbrauch wahrgenommen, zum Beispiel um unliebsame politische Meinungen zu unterdrücken. In diesem Zusammenhang wurde während der Diskussionen mehrfach der Missbrauch von Überwachungstechnologien durch die damalige ägyptische Regierung während des arabischen Frühlings erwähnt. Dieses Missbrauchspotential wird als stark angesehen, vor allem aufgrund des wahrgenommenen Fehlens von Transparenz, vor allem im Hinblick auf Datenerhebung, Datensicherheit, verantwortliche Stelle, Speicherdauer und die Zwecke der Datenverarbeitung. Eine Sorge, die oft erwähnt wurde, war die Speicherung erstmal gesammelter Daten unter Umständen für eine lange Zeit, so dass diese gegebenenfalls zu anderen Zwecken weiterverwendet werden könnten. Aus diesem Grunde wünschten sich etliche Teilnehmer wiederholt, dass es Maßnahmen für mehr Transparenz und Kontrolle staatlicher Stellen, die intelligente Videoüberwachung nutzen, geben möge.

Handyortung

Hinsichtlich der Handyortung ergaben die Fragen mit nur leichten Abweichungen ein ähnliches Bild wie bei der intelligenten Videoüberwachung. Insgesamt 39,8 % sagten, die Aussage, dass die Handyortung ein wirksames Mittel für die öffentliche Sicherheit sei, träfe eher nicht oder überhaupt nicht zu, wohingegen insgesamt 27,4 % meinten, dies sei eher oder vollständig zutreffend. Im Gegensatz zur intelligenten Videoüberwachung sah hier ein größerer Prozentsatz von 32,3 % die Aussage differenziert.

Im Vergleich mit intelligenter Videoüberwachung stimmte eine deutlich geringere Zahl von Teilnehmern der Aussage zu, dass sie sich durch Handyortung unbehaglich fühlen würden (Q28: 59,4 %). Dahingegen widersprachen lediglich 23,5 % insgesamt dieser Aussage. Im Einklang mit diesen Ergebnissen sagten insgesamt 60,1 %, es träfe eher nicht oder überhaupt nicht zu, dass sie sich durch den Einsatz von Handyortung sicherer fühlen würden. In diesem Zusammenhang meinten nur 16,5 % der Teilnehmer, dass sie sich sicherer fühlen würden, wenn diese Technologie zum Einsatz käme. Bemerkenswert ist hierbei die auffällig große Zahl von Teilnehmern (22,9 %), die diese Aussage differenziert sahen.

Handyortung

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Meiner Meinung nach ist Handyortung ein wirksames Mittel für die öffentliche Sicherheit.	Q27	186	11,8 %	15,6 %	32,3 %	21,5 %	18,3 %	0,5 %
Handyortung bereitet mir Unbehagen.	Q28	187	33,2 %	26,2 %	17,1 %	13,9 %	9,6 %	0,0 %
Ich fühle mich sicherer, wenn Handyortung eingesetzt wird.	Q29	188	6,9 %	9,6 %	22,9 %	28,7 %	31,4 %	0,5 %
Ich habe den Eindruck, dass mir Handyortung ohne meine Einwilligung aufgezwungen wird.	Q30	187	60,4 %	21,4 %	7,5 %	2,7 %	7,0 %	1,1 %
Handyortung ist ein angemessenes Mittel, um nationale Sicherheitsbedrohungen zu	Q31	189	5,8 %	12,2 %	25,4 %	25,9 %	29,1 %	1,6 %

bewältigen.								
Handyortung beunruhigt mich nicht, solange sie nur auf Kriminelle abzielt.	Q38	184	13,0 %	8,7 %	9,8 %	19,0 %	42,4 %	7,1 %
Ich bin besorgt, wie sich der Einsatz von Handyortung künftig weiterentwickeln könnte.	Q39	187	62,6 %	13,9 %	11,2 %	7,0 %	4,3 %	1,1 %
Handyortung beunruhigt mich nur, wenn sie eingesetzt wird, um mein eigenes Mobiltelefon zu überwachen.	Q40	185	5,4 %	4,3 %	7,0 %	11,4 %	66,5 %	5,4 %

Tabelle 12: Wahrgenommene Wirksamkeit von Handyortung

Wie bei der intelligenten Videoüberwachung nimmt eine recht große Zahl von Teilnehmern (Q30: 81,8 % mit den Antwortoptionen "Trifft eher zu" und "Trifft vollständig zu") die Handyortung als aufgezwungen wahr, während nur 9,7 % diesen Eindruck nicht haben. Im Vergleich zur Kameraüberwachung widersprach ein Prozentsatz von 55,0 % der Aussage, dass die Handyortung ein angemessenes Mittel sei, um nationale Sicherheitsbedrohungen zu bewältigen. Dahingegen drückten 18,0 % ihre Zustimmung hierbei aus und 25,4 % sahen die Frage, ob Handyortung geeignet sei, um Sicherheitsbedrohungen zu adressieren, differenziert.

Verglichen mit intelligenter Videoüberwachung kam der Teil über die Handyortung zu ähnlichen Ergebnissen, sofern es um die Wahrnehmung der Bürger hinsichtlich des Abzielens dieser Technologie nur auf Kriminelle ging. Insgesamt 61,4 % sagten, das gegebene Statement (Q38) träfe eher nicht oder überhaupt nicht zu während 7,1 % eine differenzierte Einschätzung abgaben und 21,7 % der Aussage zustimmten. Ähnlich wie bei der intelligenten Videoüberwachung wählte hierbei eine leicht erhöhte Anzahl von Teilnehmern die Antwortoption "Keine Angabe" (7,1 %).

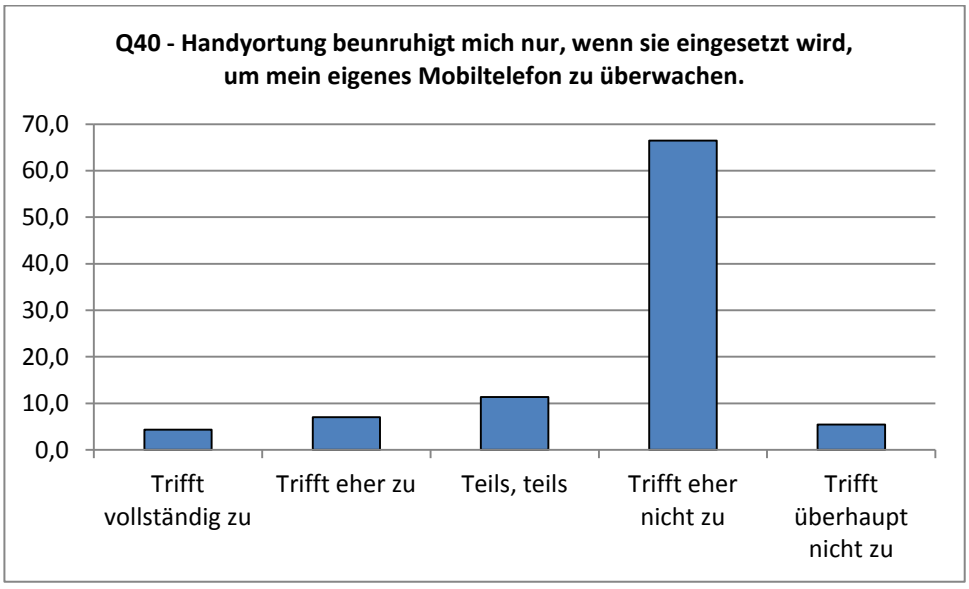

Abbildung 6: Bedeutung persönlicher Betroffenheit in Bezug auf Handyortung

Mit insgesamt 76,5 % im "Trifft vollständig zu"/"Trifft eher zu" Spektrum drückte eine (im Vergleich zur intelligenten Videoüberwachung) größere Mehrheit von Teilnehmern ihre Besorgnis hinsichtlich der zukünftigen Entwicklung dieses Technologieeinsatzes aus, während 11,9 % dies nicht so sahen (Q39). Vergleichbar wie bei der intelligenten Videoüberwachung wäre ein recht hoher Prozentsatz der Antwortenden von 77,9 % beunruhigt durch Handyortung, sogar wenn nicht das eigene Mobiltelefon betroffen ist. Nur 9,7 % gaben an, dass sie dann nicht beunruhigt seien. Die Meinung der Bürger in Bezug auf die Beeinträchtigung der Privatsphäre durch

Handyortung unterscheidet sich jedoch in ihren Ergebnissen deutlich von jenen zur intelligenten Videoüberwachung (siehe Tabelle unten).

Q80 - Wählen Sie jene Aussage, die Ihrer Meinung am besten entspricht (N= 185)

Handyortung ist sinnvoll und greift nicht besonders tief in die Privatsphäre ein.	13,0 %
Handyortung ist sinnvoll, greift aber tief in die Privatsphäre ein.	56,2 %
Handyortung ist nutzlos und greift tief in die Privatsphäre ein.	23,2 %
Handyortung ist weder sinnvoll noch greift es in die Privatsphäre ein.	1,1 %
Keine Angabe	6,5 %

Tabelle 13: Wahrgenommene Eingriffsintensität von Handyortung

Hier ist die Handyortung mehrheitlich als nützlich, aber dennoch tief in die Privatsphäre eingreifend angesehen worden (56,2 %), während ein kleinerer Prozentsatz von 23,2 % diese Technologie als nutzlos neben die Privatsphäre beeinträchtigend ansieht. Im Vergleich zur intelligenten Videoüberwachung sieht zudem eine größere Zahl von Teilnehmern (13,0 %) die Handyortung sowohl als nützlich, als auch die Privatsphäre nicht beeinträchtigend an.

Während der Gruppendiskussionen sagten die teilnehmenden Bürger, dass aus ihrer Perspektive die Handyortung am meisten in Einzelfällen für spezifisch de nütze. Im Bereich der Privatwirtschaft bilden sogenannte Tracking-Funktionen die Grundlage einer Vielzahl nützlicher Dienste, wie etwa Navigation oder Ortsempfehlungen. Als Beispiel für die staatliche Nutzung von Ortungswerkzeugen wurde das Auffinden vermisster und hilfloser Personen (wie etwa Kinder, Ältere oder behinderte Menschen) genannt. Zudem könne eine Ortung im Falle von Unglücksfällen oder bei Kriminalitätsopfern, wie auch gestohlenen Mobilgeräten, sinnvoll sein. Die Ortung konkreter Verdächtiger wurde ebenfalls genannt. Weiterhin wurde anerkannt, dass eine Ortung im Falle des Transports von gefährlichen oder wertvollen Gütern nützlich sein kann. Über diese mehrfach genannten Beispiele hinaus sagten einige Teilnehmer auch, dass Handyortung helfen könne, Serienstraftaten aufzuklären sowie als unterstützendes Beweismaterial in Strafverfahren dienen könnte oder sogar den entlastenden Beweis erbringen könne, dass sich ein Verdächtiger zum Tatzeitpunkt nicht am Tatort aufgehalten hat.

Jedoch hatten die Bürger auch ernsthafte Einwände gegen den Einsatz von Handyortung als Sicherheitsmaßnahme. Die Wirksamkeit als präventives Mittel wurde angezweifelt; ebenso die Eignung als Beweismittel, da die Informationen über den Standort eines Mobiltelefons vor Gericht nur als Indiz für eine Straftat dienen könne. Generell wurde angenommen, dass professionelle Straftäter das Mittel der Handyortung kennen und diese umgehen könnten. Das rechtliche Rahmenwerk wurde als manchmal unzureichend empfunden, und manche Teilnehmer forderten eine wirksamere und kompetentere Anwendung gerichtlicher Kontrolle.

Ähnlich wie bei intelligenter Videoüberwachung wurde die Streubreite der Maßnahme stark kritisiert. Insbesondere Funkzellenabfragen wurden als unverhältnismäßige Rasterfahndung angesehen, welche einen Generalverdacht in Bezug auf viele unschuldige Bürger impliziere. In Bezug auf politische Demonstrationen und die verfassungsmäßig garantierte Versammlungsfreiheit wurde Handyortung als Mittel der Abschreckung wahrgenommen, das ein Gefühl des Überwachtseins und Machtlosigkeit vermittelt. Oft erwähnt wurde die Möglichkeit, Bewegungsprofile von Personen zu erstellen, welche intime und sensible Details aus deren alltäglichen Leben und deren sozialem Umfeld preisgeben könnte. In diesem Zusammenhang war das Missbrauchspotential Gegenstand vieler Diskussionen. Viele Teilnehmer wünschten sich mehr Transparenz über Datenerhebung, Speicherdauer, Zwecke und Analysekriterien.

3.2.2 Vermeidung von und Widerstand gegen Überwachung

Die Ergebnisse des Bürgerforums zeigen ein recht vielschichtiges Bild der kritischen Einstellung gegenüber den betrachteten Sicherheitstechnologien. Im Kontext intelligenter Videoüberwachung zeigen die Ergebnisse von Q57, dass 20,1 % der Bürger sich aktiv gegen die Nutzung dieser Technologien einsetzen würden, während sogar 23,9 % angaben, auf jeden Fall bereit zu sein, die Nutzung zu verhindern. Zumindest 10,9 % würden andere beim Protest gegen den Einsatz

intelligenter Videoüberwachung unterstützen. Jedoch wurde von einer recht großen Zahl von Teilnehmern (33,7 %) ein weniger aktiver Ansatz gegen diese Sicherheitstechnologie bevorzugt, indem sie angaben, sie würden gerne mehr darüber wissen, wie sie sich vor intelligenter Videoüberwachung schützen könnten. Nur 8,7 % der Bürger gaben an, dass sie überhaupt nichts gegen intelligente Videoüberwachung einzuwenden hätten. Im Zusammenhang mit Handyortung zeigen die Ergebnisse zu Q59, dass sich 17,1 % aktiv gegen den Einsatz dieser Technologie einsetzen würden. 19,3 % der Teilnehmer gaben sogar an, auf jeden Fall bereit zu sein, sich aktiv gegen Handyortung einzusetzen; 10,5 % würden andere bei ihrem Protest gegen Handyortung unterstützen. Im Vergleich mit den Antworten bei der intelligenten Videoüberwachung gab es sogar eine größere Mehrheit von 40,9 %, die angab mehr erfahren zu wollen, wie sie sich gegen Handyortung schützen könnten. Nur 8,8 % der Bürger sagten, sie hätten überhaupt nichts gegen Handyortung einzuwenden.

Bei dem Bürgerforum in Deutschland wurden die Teilnehmer zu beiden Technologien auch gefragt, inwieweit sie aktiv vermeiden, von diesen überwacht bzw. verfolgt zu werden (intelligente Videoüberwachung = Q60 und Handyortung = Q62). Eine bemerkenswert hohe Anzahl von Bürgern gab an, sie würden ihr Verhalten ändern, sobald sie sich bewusst seien, überwacht zu werden. Diese Antwort wurde für beide betrachteten Technologien von ähnlich vielen Teilnehmern gegeben, 31,3 % bei der intelligenten Videoüberwachung und 38,0 % bei der Handyortung. Im Falle der intelligenten Videoüberwachung des öffentlichen Raums sagte noch eine recht große Zahl von Teilnehmern (insgesamt 39,6 %), dass sie ihr Verhalten deswegen nicht ändern würden. Jedoch gaben demgegenüber 23,1 % an, sie würden es vermeiden, in Gegenden zu gehen, wo intelligente Kameraüberwachung eingesetzt wird. Nur eine kleine Zahl von Bürgern (1,6 %) gab an, sie würden nie in Gegenden gehen, in denen intelligente Videoüberwachung eingesetzt wird. Die Antworten auf die entsprechenden Fragestellungen bei der Handyortung weisen ähnliche Ergebnisse auf, wobei insgesamt 34,2 % angaben, sie würden vermutlich nicht oder ganz sicher nicht ihr Verhalten infolge des Einsatzes dieser Technologie ändern. Jedoch antworteten 13,6 %, sie würden aufgrund des Einsatzes von Handyortung aktiv vermeiden, ein Mobilfunkgerät zu nutzen und sogar 8,2 % gab an, deswegen nie ein Mobiltelefon zu gebrauchen. Im Ergebnis sind dies dann insgesamt 21,8 % der teilnehmenden Bürger, die Vorbehalte haben, Mobilfunkgeräte in dem Bewusstsein der Möglichkeit zu nutzen, geortet und verfolgt zu werden.

Während der Gruppendiskussionen wurde deutlich, dass vor allem die jüngeren Teilnehmer recht versiert bei der Nutzung moderner Technologien wie dem Internet oder Smartphones sind. Dies umfasst auch recht detailliertes Wissen über die Strategien von Privatfirmen wie auch staatlichen Institutionen im Hinblick auf Datenerhebung und Überwachung zu den unterschiedlichsten Zwecken. Diese Teilnehmer gaben jedoch auch zu, sich als sogenannte digital natives an das Gefühl von Beobachtung und Überwachung sowie daran gewöhnt zu haben, auf der Basis eigener, freiwillig oder unfreiwillig preisgegebener Daten bewertet zu werden. In einem Fall sagte eine junge Teilnehmerin, sie sei an das Gefühl staatlicher Überwachung gewöhnt, da sie in der früheren DDR aufwuchs, wo ihre Eltern von der Stasi überwacht worden und Akten über ihre Familie angelegt worden seien. Mit dem Hintergrund der deutschen historischen Erfahrungen aus dem Naziregime und der DDR gaben vor allem die älteren Teilnehmer an, zögerlicher bei der Akzeptanz überwachungsbasierter Sicherheitstechnologien zu sein. Als konsequente Folge sagten gerade diese älteren Teilnehmer bei dem Bürgerforum, dass sie bewusst die Nutzung moderner Technologien im Allgemeinen vermeiden, auch wenn zugestanden wurde, dass diese manchmal einen gewissen Komfort bieten. In manchen Fällen gaben Bürger an, dass sie die Nutzung solcher Technologien vollständig eingestellt hätten, da sie sich infolge der möglichen umfangreichen Erhebung ihrer Daten unbehaglich fühlten. Nur einige wenige Bürger gaben die Aussage "wer nichts zu verbergen hat, hat nichts vor Überwachung zu befürchten". Jedoch widersprach die Mehrheit der teilnehmenden Bürger genau diesem Statement mit dem Argument, dass auch jeder Unschuldige unfreiwillig das Ziel von Überwachung werden könne.

3.2.3 Wahrnehmung individueller und kollektiver Aspekte

In diesem Abschnitt wird die Sichtweiseder Bürger sowohl aus persönlicher Sicht wie auch aus einer mehr kollektiven oder gesellschaftlichen Perspektive betrachtet. Insgesamt kann festgestellt werden, dass Privatsphäre als Begrifflichkeit, wie auch als umfassendes Konzept, für viele Bürger

sehr unterschiedliche Bedeutung haben kann. Wo manche die Privatsphäre als ein Konzept sehen, welches lediglich auf den Schutz des Einzelnen fokussiert ist, nehmen andere eine allgemeinere Perspektive ein, in der Annahme, dass die Privatsphäre bzw. das Recht auf informationelle Selbstbestimmung einen größeren gesellschaftlichen Wert jenseits der individuellen Kontrolle über eigene personenbezogene Informationen hat. Die geäußerten Meinungen zeigten ein vielschichtiges Bild der Teilnehmer über die jeweiligen Nutzungszwecke und Missbrauchsrisiken (siehe Tabelle unten).

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Der Einsatz von überwachungs-basierten Sicherheits-technologien verbessert die öffentliche Sicherheit.	Q84	180	5,6 %	10,0 %	32,8 %	26,7 %	25,0 %	0,0 %
Überwachungsbasierte Sicher-heitstechnologien werden nur eingesetzt, um zu zeigen, dass etwas zur Verbrechens-bekämpfung getan wird.	Q85	182	14,3 %	20,9 %	18,1 %	20,9 %	21,4 %	4,4 %
Wer nichts Falsches macht, muss wegen überwachungs-basierter Sicherheits-technologien nicht besorgt sein.	Q86	185	5,4 %	5,9 %	8,1 %	14,1 %	64,3 %	2,2 %
Wenn überwachungsbasierte Sicherheitstechnologien verfügbar sind, dann ver-wenden Regierungen diese auch.	Q87	182	70,3 %	17,6 %	9,3 %	1,1 %	0,5 %	1,1 %
Sobald überwachungsbasierte Sicherheitstechnologien eingeführt sind, ist der Missbrauch wahrscheinlich.	Q88	185	56,2 %	27,6 %	10,3 %	4,3 %	0,0 %	1,6 %
Insgesamt bin ich der Ansicht, dass überwachungs-basierte Sicherheitstechnologien routinemäßig eingesetzt werden sollen, um die öffent-liche Sicherheit zu verbessern.	Q94	183	8,7 %	11,5 %	19,1 %	22,4 %	37,7 %	0,5 %

Tabelle 14: Einstellung zu den Technologien im Allgemeinen

Die Ergebnisse zeigen, dass eine große Mehrheit meint, dass Überwachungstechnologien von Regierungen auch benutzt werden, sobald sie verfügbar sind (87,9 % insgesamt). Sowohl zu Beginn der Veranstaltung (Q7) als auch zu deren Ende (Q94) wurden die Teilnehmer gefragt, ob ihrer Meinung nach Sicherheitstechnologien routinemäßig eingesetzt werden sollen, um die öffentliche Sicherheit zu verbessern. Die Zustimmung zu dieser Aussage war bereits zu Beginn der Veranstaltung gering und ist zum Ende der Veranstaltung gesunken. Dies könnte darauf zurückzuführen sein, dass die Auswirkungen der Technologien in den gezeigten Filmen dargestellt und von den Teilnehmern in den Gruppendiskussionen aufgegriffen worden sind.

Während der Diskussionen wurde betont, dass die deutsche Regierung verpflichtet sei, die Privatsphäre/Freiheit genauso wie die Sicherheit zu schützen, wobei erstere für eine ganze Weile zu stark vernachlässigt worden seien. Deutsche Politiker werden so wahrgenommen, als ob sie sich zu stark auf den Aspekt öffentlicher Sicherheit konzentrieren und sich hierbei auf Dinge fokussieren, die faktisch weit weniger risikoreich seien, als sie in der Politik und in den Medien dargestellt würden. Als oft genanntes Beispiel wurde erwähnt, dass sich Politiker oftmals auf die Gefahr schwerer Verbrechen und Terrorismus konzentrieren würden, während Verkehrsunfälle

und Klimawandel eigentlich größere Sicherheitsbedrohungen für die Bürger in Deutschland darstellen würden. Allgemein sagten die Bürger, dass sich Politiker und andere Entscheidungsträger zu sehr auf vage Versprechen moderner Technologien ohne fundierte wissenschaftliche Grundlage verlassen, während sie kritisierten, dass die Sicherheitsindustrie einen zu großen Einfluss auf die deutsche Regierung hätte.

Hinsichtlich der Perspektive auf die persönlichen Auswirkungen im Vergleich zu den eher generellen gesellschaftlichen Konsequenzen solcher Technologien hatten die Bürger ebenfalls ein sehr facettenreiches Bild. Wenn man die Ergebnisse der diesbezüglichen Fragestellungen betrachtet, erscheint es offensichtlich, dass sich Bürger nicht nur persönlich betroffen fühlen, sondern auf hinsichtlich der gesellschaftlichen Auswirkungen von Überwachungstechnologien besorgt sind (Q95).

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Ich bin besorgt, dass zu viele Informationen über mich gesammelt werden.	Q89	183	71,0 %	14,2 %	7,7 %	4,9 %	1,1 %	1,1 %
Ich bin besorgt, dass die über mich gespeicherten Informationen nicht korrekt sind.	Q90	181	37,6 %	20,4 %	19,3 %	9,4 %	5,5 %	7,7 %
Ich bin besorgt, dass meine persönlichen Informationen ohne meine Zustimmung weitergegeben werden.	Q91	178	83,7 %	8,4 %	5,6 %	1,1 %	0,6 %	0,6 %
Ich bin besorgt, dass meine persönlichen Informationen gegen mich verwendet werden können.	Q92	183	57,9 %	21,9 %	8,7 %	7,1 %	2,2 %	2,2 %
Ich bin besorgt, dass der Einsatz von überwachungsbasierten Sicherheitstechnologien die Privatsphäre im Allgemeinen aushöhlt.	Q95	182	63,7 %	15,4 %	8,8 %	6,0 %	4,4 %	1,6 %
Ich bin besorgt, dass der Einsatz von überwachungs-basierten Sicherheitstechnologien meine Privatsphäre aushöhlt.	Q96	183	65,0 %	16,4 %	7,1 %	7,1 %	3,8 %	0,5 %

Tabelle 15: Individuelle und generelle Bedenken

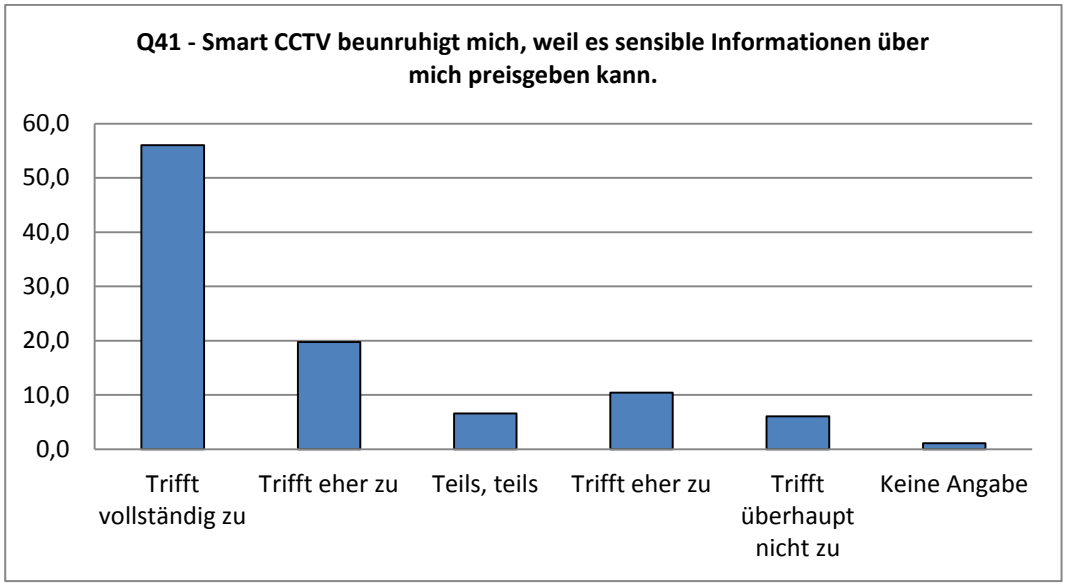

Abbildung 7: Bedenken in Bezug auf das Risiko für sensible Daten bei intelligenter Videoüberwachung

Ferner zeigen die Abbildung oben und die Tabelle unten, dass die Bürger Sorgen haben, dass durch die Technologien sensible Informationen über sie preisgegeben werden und dass ihr Verhalten fehlinterpretiert werden kann.

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Smart CCTV beunruhigt mich, weil es sensible Informationen über mich preisgeben kann.	Q41	182	56,0 %	19,8 %	6,6 %	10,4 %	6,0 %	1,1 %
Smart CCTV beunruhigt mich, weil es Unbekannten zeigen kann, wo ich bin,	Q42	185	59,5 %	19,5 %	8,6 %	7,6 %	2,2 %	2,7 %
Smart CCTV beunruhigt mich, weil es zu Fehlinterpretationen meines Verhaltens führen kann,	Q43	186	68,3 %	11,3 %	7,0 %	7,5 %	3,8 %	2,2 %
Smart CCTV beunruhigt mich, weil es meine Grundrechte verletzen kann,	Q44	182	63,7 %	11,0 %	8,8 %	7,1 %	7,1 %	2,2 %
Smart CCTV beunruhigt mich, weil es unser aller Grundrechte verletzen kann,	Q45	180	64,4 %	15,0 %	7,2 %	6,7 %	5,0 %	1,7 %

Tabelle 16: Intelligente Videoüberwachung – Sensible Daten, Verhaltensinterpretation und Bedenken hinsichtlich Grundrechtsbeeinträchtigungen

Die kollektiven Aspekte erfahren gegenüber den individuellen Aspekten mehr Aufmerksamkeit von den Bürgern, was sich aus den abweichenden Prozentwerten bei den Antworten zu Q44 und Q45 ergibt. Während 74,7 % der Bürger wegen möglicher negativer Auswirkungen von intelligenter Videoüberwachung auf ihre Grundrechte besorgt sind, ist diese Zahl mit 79,4 % etwas höher, wenn es um die Grundrechte aller Bürger geht.

Die Ergebnisse zur Handyortung erlauben eine ähnliche Auswertung. Schon in den Tabellen 12 und 13 in Kapitel 3.2.1 wurde die Beeinträchtigung der individuellen Privatsphäre als erheblich angesehen, während gesellschaftliche Aspekte ebenfalls eine Rolle spielten. Dies wird ergänzt durch die geäußerten Bedenken im Hinblick auf die mögliche Enthüllung sensibler Informationen und den Standort von Bürgern durch Handyortung (siehe Tabelle unten). Schlussendlich gibt es

starke Bedenken gegen Handyortung aus der Befürchtung heraus, dass es Fehlinterpretationen von Verhalten geben könnte. Etwa 74,0 % der Bürger sind besorgt, dass ihr Verhalten fehlinterpretiert werden könnte, wenn sie durch von Sicherheitsbehörden eingesetzte Handyortung betroffen sind.

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Handyortung beunruhigt mich, weil sie sensible Informationen über mich preisgeben kann.	Q52	187	52,9 %	20,3 %	14,4 %	7,0 %	5,3 %	0,0 %
Handyortung beunruhigt mich, weil sie Unbekannten zeigen kann, wo ich bin (oder war).	Q53	186	62,4 %	17,2 %	10,2 %	5,9 %	3,2 %	1,1 %
Handyortung beunruhigt mich, weil sie zu Fehlinterpretationen meines Verhaltens führen kann.	Q54	185	55,1 %	18,9 %	10,8 %	8,1 %	5,4 %	1,6 %
Handyortung beunruhigt mich, weil sie meine Grundrechte verletzen kann.	Q55	187	58,8 %	19,8 %	5,9 %	8,0 %	7,0 %	0,5 %
Handyortung beunruhigt mich, weil sie unser aller Grundrechte verletzen kann.	Q56	186	59,7 %	16,7 %	8,1 %	7,0 %	7,0 %	1,6 %

Tabelle 17: Handyortung – Sensible Daten, Verhaltensinterpretation und Bedenken hinsichtlich Grundrechtsbeeinträchtigungen

Die gesellschaftlichen Aspekte werden auch deutlich, sobald es um Grundrechte des Einzelnen, wie auch im Allgemeinen geht. Im Gegensatz zur intelligenten Videoüberwachung gibt es hier leichte Unterschiede in der Gewichtung der gesellschaftlichen Aspekte. Während die Besorgnis über die gesellschaftlichen Auswirkungen noch immer stark ist (76,4 %), erscheint die persönliche Betroffenheit durch die Handyortung etwas wichtiger für die Bürger. Für 78,6 % trifft es vollständig oder eher zu, dass Handyortung die eigenen Grundrechte verletzen könnte. Jedoch ist, ähnlich, wie bei der intelligenten Videoüberwachung, die kritische Haltung bei beiden Aspekten stark vertreten.

Unabhängig von den Technologien behandelten die Gruppendiskussionen sowohl persönliche als auch gesellschaftliche Aspekte der Erosion der Privatsphäre. Nach Auffassung einiger Teilnehmer müsse ein demokratischer Staat die Grundrechte seiner Bürger schützen und hierbei bis zu einem gewissen Maß Unsicherheit in Kauf nehmen, um seine Natur zu bewahren. Durch breiteste Überwachungsaktivitäten staatlicher Stellen werde das Vertrauen in den Staat unterminiert, weil sich seine Bürger einem Generalverdacht ausgesetzt sähen. Breit gestreute Überwachungsmaßnahmen, die große Teile der Bevölkerung betreffen, wurden als unverhältnismäßige schleichende Ausweitung der Zweckbestimmung angesehen. Dies könne in eine faktische Erosion der verfassungsmäßig garantierten Unschuldsvermutung münden. Infolgedessen würden die Bürger einen Abschreckungseffekt auf ihr Verhalten spüren, angetrieben von dem Wunsch, in Ruhe gelassen zu werden. Viele Bürger sagten bei der Veranstaltung, dass sie die zunehmende Nutzung von Überwachungstechnologien wie einen sogenannten "Big Brother" wahrnehmen würden, der eine Atmosphäre des Misstrauens schaffe, die bereits in der deutschen Geschichte durchlebt wurde.

3.3 Vertrauenswürdigkeit von Sicherheitsbehörden und die Rolle alternativer Sicherheitskonzepte

Wie bereits oben dargestellt, äußerten die teilnehmenden Bürger bei dem Bürgerforum sehr kritische Meinungen hinsichtlich der Beeinträchtigung durch Sicherheitstechnologien. Dennoch wurden diese Technologien grundsätzlich als Mittel angesehen, die eventuell geeignet seien,

Sicherheitsverbesserungen herbeizuführen, aber ein gewisses Missbrauchspotential haben. Daher wurde deutlich, dass die Art und Weise, wie diese Technologien letztlich genutzt werden, ein entscheidender Faktor für deren Akzeptanz ist. Infolgedessen ist die Vertrauenswürdigkeit jener Institutionen, die solche Sicherheitstechnologien einsetzen, ein Schlüsselfaktor. Die Einsatzzwecke, der Anwendungsbereich und die konkrete Umsetzung der Nutzung sind Argumente, welche die Bürger genau unter die Lupe nehmen, um die Verhältnismäßigkeit behördlichen Handelns zu bestimmen, denen die Sicherheit der Bürger in Deutschland anvertraut ist.

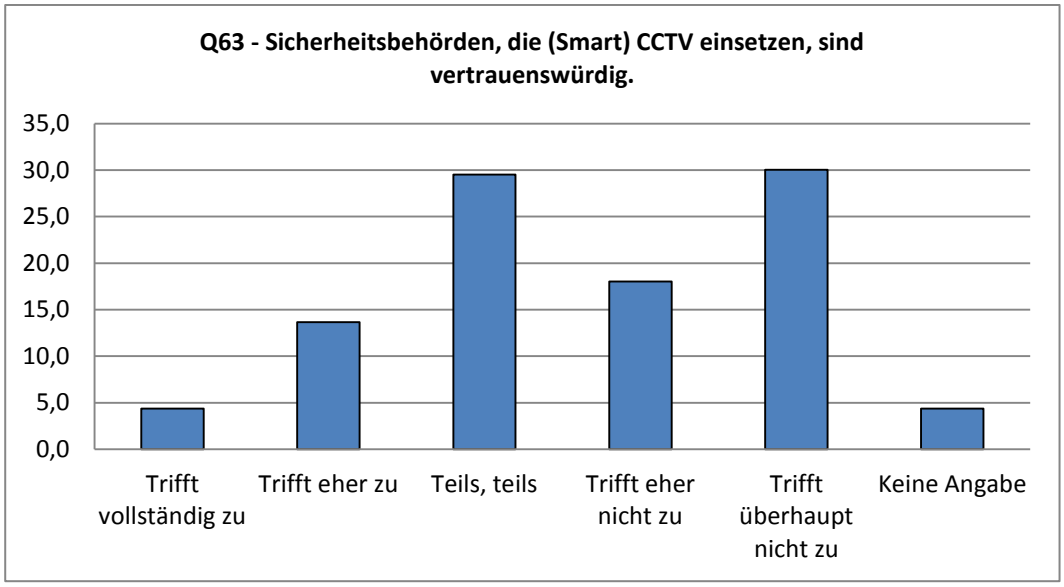

Abbildung 8: Wahrgenommene Vertrauenswürdigkeit von Institutionen die intelligente Videoüberwachung einsetzen

Soweit die Sicherheitstechnologien diskutiert wurden, drückten einige Bürger Zweifel hinsichtlich der Vertrauenswürdigkeit und der Kompetenz der einsetzenden Behörden aus. Im Hinblick auf intelligente Videoüberwachung gaben nur 18,1 % an, es träfe vollständig oder eher zu, dass diese Technologie einsetzende Sicherheitsbehörden vertrauenswürdig seien. Die Abbildung oben visualisiert diese von den Bürgern gefühlte Ambivalenz hinsichtlich der Vertrauenswürdigkeit staatlicher Institutionen, die intelligente Videoüberwachung einsetzen. Diese Ambivalenz unterstreicht, dass Vertrauenswürdigkeit für die Bürger eine wichtige Angelegenheit zu sein scheint. Noch geringere Zustimmung zeigte die Bewertung der Kompetenz, wobei nur 9,9 % der Bürger meinen, dass Sicherheitsbehörden kompetent genug sind, diese Technologie zu nutzen.

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Sicherheitsbehörden, die (Smart) CCTV einsetzen, sind vertrauenswürdig.	Q63	183	4,4 %	13,7 %	29,5 %	18,0 %	30,1 %	4,4 %
Sicherheitsbehörden, die (Smart) CCTV einsetzen, sind kompetent in ihrer Tätigkeit.	Q64	181	2,2 %	7,7 %	32,6 %	24,9 %	26,0 %	6,6 %
Sicherheitsbehörden, die (Smart) CCTV einsetzen, sind besorgt um das Wohlergehen der BürgerInnen und um die öffentliche Sicherheit.	Q65	183	5,5 %	19,1 %	31,1 %	16,9 %	21,3 %	6,0 %
Sicherheitsbehörden, die (Smart) CCTV einsetzen, missbrauchen ihre Macht nicht.	Q66	182	4,9 %	11,0 %	25,8 %	18,7 %	34,1 %	5,5 %

Tabelle 18: Vertrauenswürdigkeit von Sicherheitsbehörden im Gesamtkontext der Nutzung intelligenter Videoüberwachung

Auch über die allgemeine Vertrauenswürdigkeit hinaus und die Befähigung, die Technologie richtig zu nutzen, offenbaren die Ergebnisse ein tiefes Misstrauen hinsichtlich der Rechtstaatlichkeit der Sicherheitsbehörden, die überwachungsbasierte Maßnahmen einsetzen. Weniger als ein Viertel der Teilnehmer (24,6 % im "Trifft vollständig zu/Trifft eher zu" Spektrum) meint, dass die Zielrichtung solcher Behörden das Wohlergehen der Bürger und der Schutz der öffentlichen Sicherheit ist. Außerdem wurde das Missbrauchsrisiko recht hoch eingeschätzt. Mehr als die Hälfte der Teilnehmer (insgesamt 52,8 %) hält es für möglich, dass Sicherheitsbehörden ihre Macht missbrauchen, die ihnen diese Technologie gibt.

Q75 - Wählen Sie jene Aussagen, die Ihrer Meinung am ehesten entsprechen (max. 4 Antworten), (N= 176)

Ich glaube, Gesetze und Vorschriften gewährleisten dass Smart CCTV nicht missbraucht wird.	13,6 %
Ich glaube dass Smart CCTV die öffentliche Sicherheit erhöht.	35,2 %
Ich glaube dass Smart CCTV in die Privatsphäre eingreift.	84,7 %
Ich glaube dass im Hinblick auf die möglichen Vorteile das Ausmaß des Eingriffs akzeptabel ist.	23,3 %
Nichts vom oben Genannten	1,7 %
Keine Angabe	1,7 %

Tabelle 19: Meinungen zu intelligenter Videoüberwachung

Das bekundete Misstrauen der Teilnehmer in staatliche Sicherheitsbehörden wird wie die Antworten auf Frage 75 zeigen, nicht durch ein Vertrauen in rechtliche Beschränkungen zur Nutzung der Sicherheitstechnologien aufgefangen, ebenso wenig durch tatsächliche faktische Vorteile kompensiert. Während nur 13,6 % der Teilnehmer glauben, dass Gesetze und Vorschriften geeignet sind, um das Missbrauchsrisiko einzuschränken, fokussierte sich eine große Zahl von Teilnehmern (84,7 %) stark auf die Beeinträchtigung durch diese Maßnahme. Dennoch erkennen einige Bürger an (35,2 %), dass intelligente Videoüberwachung das Potential hat, die Sicherheit zu verbessern. Wird jedoch die starke Wahrnehmung der Beeinträchtigung mit einbezogen, sehen nur 23,3 % diese Technologie als nützlich genug an, um sie als standardmäßige Sicherheitsmaßnahme zu akzeptieren.

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Insgesamt befürworte ich die Einführung von Smart CCTV als öffentliche Sicherheitsmaß-nahme.	Q81	182	5,5 %	8,2 %	19,8 %	17,0 %	48,4 %	1,1 %

Tabelle 20: Generelle Unterstützung intelligenter Videoüberwachung als Sicherheitslösung

Dies resultiert in einer recht geringen Unterstützung von intelligenter Videoüberwachung als Sicherheitslösung mit einem Prozentwert von 13,7 %. Im Vergleich mit der intelligenten Videoüberwachung zeigen die Ergebnisse zur Handyortung eine weniger kritische Haltung hinsichtlich der einsetzenden Sicherheitsbehörden, wobei die Ergebnisse noch immer eine gedämpfte Haltung der Teilnehmer zu diesen Fragen offenbaren (siehe Tabelle unten).

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Sicherheitsbehörden, die	Q71	185	7,6 %	14,1 %	35,7 %	18,4 %	21,1 %	3,2 %

Handyortung einsetzen, sind vertrauenswürdig.								
Sicherheitsbehörden, die Handyortung einsetzen, sind kompetent in ihrer Tätigkeit.	Q72	185	4,9 %	7,6 %	29,2 %	26,5 %	25,4 %	6,5 %
Sicherheitsbehörden, die Handyortung einsetzen, sind besorgt um das Wohlergehen der BürgerInnen und um die nationale Sicherheit.	Q73	186	5,4 %	20,4 %	32,3 %	21,5 %	14,5 %	5,9 %
Sicherheitsbehörden, die Handyortung einsetzen, missbrauchen ihre Macht nicht.	Q74	185	5,9 %	11,9 %	23,8 %	25,9 %	28,6 %	3,8 %

Tabelle 21: Vertrauenswürdigkeit von Sicherheitsbehörden im Gesamtkontext der Nutzung von Handyortung

Etwa 21,7 % nehmen an, dass Handyortung einsetzende Sicherheitsbehörden vertrauenswürdig sind, während eine geringere Zahl von 12,5 % annimmt, dass diese in jenem Technologiebereich kompetent sind. Bei der Handyortung ist das Vertrauen in die guten Absichten staatlicher Sicherheitseinrichtungen etwas höher als bei der intelligenten Videoüberwachung (hier 25,8 %), aber nichtsdestotrotz insgesamt betrachtet nicht sonderlich hoch.

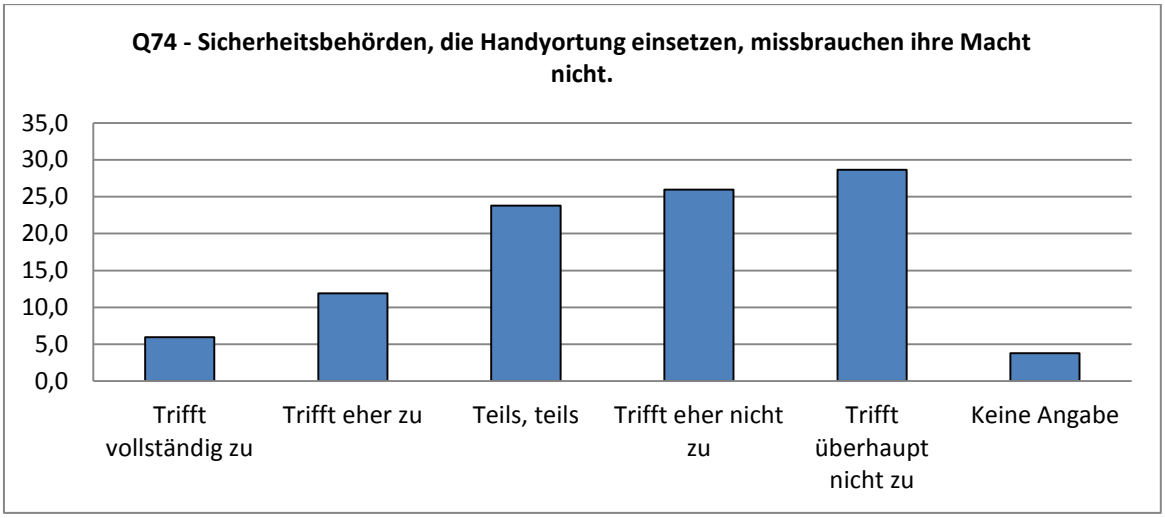

Abbildung 9: Wahrgenommenes Missbrauchspotential von Handyortung

Das Missbrauchsrisiko wurde bei der Handyortung mit 54,5 % der Bürger als höher eingestuft als bei der intelligenten Videoüberwachung.

Q77 - Wählen Sie jene Aussagen, die Ihrer Meinung am besten entsprechen (max, 4 Antworten),

(N= 171)

Ich glaube, Gesetze und Vorschriften gewährleisten dass Handyortung nicht missbraucht wird	14,6 %
Ich glaube dass Handyortung die öffentliche Sicherheit erhöht	33,9 %
Ich glaube dass Handyortung in die Privatsphäre eingreift	86,5 %
Ich glaube dass im Hinblick auf die möglichen Vorteile das Ausmaß des Eingriffs akzeptabel ist	25,7 %
Nichts vom oben Genannten	3,5 %
Keine Angabe	0,0 %

Tabelle 22: Meinungen zu Handyortung

Unter Berücksichtigung der rechtlichen Rahmenbedingungen und der faktischen Vorteile von Handyortung sind die Ergebnisse denen zur intelligenten Videoüberwachung recht ähnlich, mit einer leicht positiveren Note. Etwa 14,6 % gehen davon aus, dass Gesetze und Vorschriften Missbrauch verhindern können und 33,9 % denken, dass die Handyortung die öffentliche Sicherheit verbessern kann. Allerdings sieht eine größere Prozentzahl (hier 86,5 % im Vergleich zu 84,7 % bei der intelligenten Videoüberwachung) die Verfolgung von Mobilfunkgeräten als die Privatsphäre beeinträchtigend an. Die Vorteile und Nachteile abwägend, findet gerade mal etwas mehr als ein Viertel der Teilnehmer (25,7 %) diese Beeinträchtigung akzeptabel.

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Insgesamt befürworte ich die Einführung von Handyortung als öffentliche Sicherheitsmaß-nahme.	Q83	186	8,1 %	12,4 %	18,3 %	20,4 %	39,8 %	1,1 %

Tabelle 23: Generelle Unterstützung von Handyortung als Sicherheitslösung

Schlussendlich wurde Handyortung als routinemäßige Sicherheitsmaßnahme von 20,5 % der Teilnehmer unterstützt. Insgesamt kann gesagt werden, dass die Teilnehmer in Bezug auf die Nutzung überwachungsbasierter Sicherheitstechnologien durch staatliche Institutionen recht argwöhnisch sind, obgleich sie teilweise anerkennen, dass diese ein gewisses Wirksamkeitspotential haben können.

In den Gruppendiskussionen gaben viele Teilnehmer an, dass sie deutschen Politikern und staatlichen Einrichtungen im Hinblick auf Angelegenheiten der öffentlichen Sicherheit bis zu einem gewissen Grad vertrauen. Jedoch sei dieses Vertrauen weniger stark, sobald ausländische Sicherheitsbehörden und Geheimdienste involviert seien. Zusätzlich hierzu sei das ohnehin geringe Vertrauen seit dem NSA-Skandal noch weiter geschrumpft. Während des Bürgerforums drückten einige Bürger tiefe Enttäuschung über die deutsche Bundesregierung aus, welche nur verhalten auf die Enthüllung der allumfassenden Beeinträchtigung der Privatsphäre deutscher Bürger reagiert habe. Ferner wurde die Einbeziehung privater Firmen für Sicherheitsaufgaben kritisch betrachtet, da dies das staatliche Gewaltmonopol hin zu privaten Unternehmen verlagere. Da die Erhebung personenbezogener Daten sowohl im Privatsektor (für kommerzielle Zwecke) als auch von staatlicher Seite immer mehr zunehme, fühlten sich die Bürger machtlos und der Macht von Unternehmen wie auch den Möglichkeiten moderner Technologien, einhergehend mit Einschränkungen der Privatsphäre, ausgeliefert. Aber auch bei rein staatlicher Aktivität zum Schutz der öffentlichen Sicherheit vertrauten die Bürger nicht immer darauf, dass das Ergebnis für die deutsche Bevölkerung vorteilhaft sein kann. Das Missbrauchspotential wird allgemein als hoch bewertet, und obgleich ein gewisses Vertrauen in die aktuelle Regierung vorhanden ist, sehen die Teilnehmer die Möglichkeiten für zukünftigen Missbrauch durch repressive Regimes.

Um die Vertrauenswürdigkeit von Sicherheitsbehörden zu erhöhen, führten die Teilnehmer ein größeres Maß an Transparenz und unabhängiger Kontrolle als wichtige Faktoren an. Kontrollmechanismen wurden oft als Chance genannt, um das fehlende Vertrauen der Bürger in die Sicherheitsinstitutionen wiederzugewinnen. Dies beinhalte eine klare, ehrliche Wirksamkeitsevaluierung der jeweiligen Technologie wie auch ein verlässliches rechtliches Rahmenwerk, das auch wirksame Mittel der Durchsetzung vorsehen müsse. Hierbei bemerkten die Teilnehmer des Bürgerforums mehrfach, dass eine rein deutsche Lösung eventuell nicht ausreiche. Vielmehr sollten deutsche Politiker danach streben, umfassende europäische Lösungen zu entwickeln, die dem hohen Grad an Grundrechtsschutz in Deutschland im Vergleich mit anderen EU Ländern Rechnung tragen. Dabei sei es notwendig, mit der technischen Entwicklung aufzuschließen und das Wissen von deutschen Entscheidungsträgern, die mit Sicherheitspolitik betraut sind, zu verbessern.

Weiterhin wurde Privacy by Design (PbD) mehrfach in den Tischdiskussionen als ein Ansatz genannt, der den Missbrauch von Technologien verhindern könne. Als Beispiele für PbD-Maßnahmen wurden technische Möglichkeiten, die Datenerhebung auf das unbedingt notwendige Maß für den Sicherheitszweck einzuschränken, die Förderung von Online-Anonymität und die Unterstützung freier Software genannt. Allgemein fühlen sich Bürger zuversichtlicher, wenn eine Technologie so gestaltet ist, dass eine datenschutzfreundliche Nutzung ermöglicht oder gar der Missbrauch verhindert werde.

Neben diesen recht spezifischen Aspekten war es der Wunsch vieler Teilnehmer, dass deutsche Entscheidungsträger sich weniger auf technikzentrierte Sicherheitslösungen konzentrieren mögen. Wie bereits oben erläutert, vermissen viele Bürger den menschlichen Faktor, wenn es um Gegenmaßnahmen zu Sicherheitsrisiken geht. Zudem wurde gesagt, dass üblicherweise immer die spezifischen Rahmenbedingungen und Voraussetzungen des Einzelfalls eine Rolle spielen,

sobald die Nutzung von überwachungsbasierten Sicherheitstechnologien in Betracht gezogen wird.

Dies schlägt sich auch in den Ergebnissen nieder, sobald die Teilnehmer zu nichttechnischen Alternativen befragt wurden. Während schon viele Teilnehmer zu Beginn der Veranstaltung angaben, dass sie sich einen stärkeren Fokus auf nichttechnische Ansätze wünschen (70,9 % im "Trifft vollständig zu/Trifft eher zu" Spektrum, siehe die Ergebnisse für Q10 in der Tabelle unten), trat diese Haltung der Teilnehmer zum Ende des Bürgerforums hin noch verstärkt hervor.

Etwa 76,6 % der Teilnehmer gaben an, es träfe vollständig oder eher zu, dass alternative Ansätze zur Lösung von Sicherheitsproblemen höhere Priorität eingeräumt werden sollte, was einen deutlichen Anstieg zeigt.

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Alternativen Sicherheits-konzepten, die ohne techno-logische Mittel der Über-wachung auskommen, sollte mehr Beachtung geschenkt werden.	Q10	186	47,8 %	23,1 %	19,9 %	4,8 %	2,2 %	2,2 %
Alternativen Sicherheits-konzepten, die ohne techno-logische Mittel der Über-wachung auskommen, sollte mehr Beachtung geschenkt werden.	Q97	179	59,8 %	16,8 %	15,1 %	4,5 %	2,2 %	1,7 %

Tabelle 24: Priorisierung von (nichttechnischen) alternativen Ansätzen

Hierbei ist die deutlichste Veränderung über den Verlauf des Bürgerforums bei den unentschiedenen Teilnehmern zu verzeichnen, wobei es in der späteren Fragestellung zu einer größeren Anzahl von Bürgern kam, die zu den nichttechnischen Alternativen tendierten. Dies passt zu der oben dargestellten Ablehnung des Statements, dass Sicherheitstechnologien routinemäßig als Sicherheitslösung implementiert werden sollten (siehe die Ergebnisse zu Q7 und Q94 in den Kapiteln 3.1 und 3.2.3).

Die Teilnehmer gaben einige Beispiele alternativer Ansätze, wie z. B. die Investition in mehr Polizeipersonal, nichttechnische Ansätze zur Kriminalitätsprävention, politische und faktische Lösungen, um Armut und fehlende Bildung zu beseitigen. Allgemein wurde angeregt, nach noch mehr Möglichkeiten zu forschen, die geeignet sein könnten, um Sicherheitsprobleme in Deutschland zu bewältigen.

3.4 Die Empfehlungen von Bürgern an politische Entscheidungsträger

An den unterschiedlichen Tischen bei dem Bürgerforum hatten die Teilnehmer jeweils die Gelegenheit, eine Tischempfehlung zu formulieren, die an Entscheidungsträger sowohl auf europäischer wie auch auf nationaler Ebene gerichtet ist. Unter Einbeziehung der quantitativen Ergebnisse reflektierten diese Empfehlungen größtenteils die an diesem Tag geäußerten Meinungen und Bedenken der Bürger. Sie adressierten die Kernbedenken hinsichtlich Privatsphäre, Sicherheit und überwachungsbasierten Sicherheitstechnologien.

Die teilnehmenden Bürger hatten kaum Schwierigkeiten, sich per Tisch auf eine Empfehlung zu einigen. Zusätzlich hatten die Teilnehmer die Möglichkeit, auf Postkarten weitere Aspekte zu formulieren, die keinen Eingang in die gemeinschaftliche Empfehlung ihres Tisches fanden. Viele Teilnehmer nutzten diese Möglichkeit.

Während der gesamten Veranstaltung hatten die teilnehmenden Bürger verschiedene Bedenken im Hinblick auf Privatsphäre, Sicherheit und Sicherheitstechnologien geäußert. Die zentralen Bedenken waren eine stark wahrgenommene Beeinträchtigung der Grundrechte durch die

zunehmende Nutzung von überwachungszentrierten Maßnahmen wie auch das Fehlen von Transparenz, wirksamer Aufsicht und Kontrolle von einsetzenden Sicherheitsbehörden. Die Mehrheit der Teilnehmer drückte das Gefühl aus, dass sie nur wenig Einfluss auf die Tätigkeiten politischer Entscheidungsträger in Bezug auf Themen des Datenschutzes und der Nutzung von Überwachungstechnologien haben. Während der Veranstaltung sagten Bürger oftmals, dass sie sich breiter Überwachung sowohl durch die deutsche als auch durch ausländische Regierungen ausgeliefert fühlen. Folglich verlangten die Bürger mit ihren Tischempfehlungen in erster Linie weniger Überwachung. Weiterhin wünschen die Bürger hinreichende Transparenz gegenüber europäischen Bürgern, zum Beispiel durch proaktive Information und objektive Evaluation, in welchen Fällen Überwachung zu Sicherheitszwecken erforderlich und verhältnismäßig ist. Dies beinhaltet eine ernsthafte Überprüfung der Wirksamkeit der jeweiligen Technologie und ihrer Auswirkungen auf die Gesellschaft. Ferner wünschen die Bürger effektive Kontrolle von Sicherheitsinstitutionen, die solche Technologien einsetzen, und zwar durch geeignete organisatorische, technische und rechtliche Mittel.

Es wurde anerkannt, dass die Nutzung solcher Technologien manchmal notwendig sein kann. Aber nach Auffassung der Bürger sollte dies nur im Einzelfall einhergehend mit einer objektiven und umfassenden Prüfung in Betracht gezogen werden. Als zentraler Punkt wurde immer wieder in den Gruppendiskussionen erwähnt, dass es einen dringenden Bedarf für mehr Transparenz in der Sicherheitspolitik gibt. Nach Meinung der Teilnehmer sollte diese Transparenz mindestens Informationen über die Quelle, den Umfang und den Zweck einer Datenerhebung umfassen, wie auch über Art und Weise der Datenverarbeitung, Speicherdauer und Empfänger der Daten.

Neben der fehlenden Transparenz kritisierten die Bürger die oftmals bedingungslose Technikgläubigkeit der einsetzenden Stellen. Daher regen die Teilnehmer gegenüber politischen Entscheidungsträgern in Europa an, ihren Fokus zu einer objektiven Evaluation der Technologien hinsichtlich Wirksamkeit und Auswirkungen zu verschieben und alternativen Methoden zur Adressierung von Sicherheitsproblemen Raum zu geben. Mehrfach wurde erwähnt, dass viele Sicherheitsprobleme im Bereich von Kriminalität durch Armut, Mangel an Bildung und andere soziale Ungleichheiten verursacht werden. Schon während der Gruppendiskussionen wurden Anregungen gegeben, wie solche Probleme gelöst werden könnten, z. B. durch Verbesserungen im Bildungssektor oder durch Sozialprogramme. Über die Wurzeln von Kriminalität hinaus wurde vorgeschlagen, dass Haushaltsmittel anstatt für mehr Überwachungstechnologien besser zur Aufstockung von Personal bei der Polizei und anderen Sicherheitsbehörden verwendet werden sollten. Insgesamt war die allgemeine Haltung der am Bürgerforum teilnehmenden Bürger, dass ein stärkerer menschlicher Faktor nötig sei, um Sicherheitsproblemen zu begegnen.

Ferner adressierten die Empfehlungen den Bedarf an umfassenden rechtlichen Rahmenbedingungen, die über die nationalen Grenzen hinausgehen müssen, um zu gewährleisten dass verfassungsgemäß garantierte Grundrechte effektiver geschützt werden. Hierbei war die am häufigsten genannte Empfehlung die Schaffung eines harmonisierten, internationalen (zumindest EU-weiten) rechtlichen Rahmenwerks zum Schutz personenbezogener Informationen. Als Grund für diese Forderung gaben die Teilnehmer an, dass gerade im jetzigen digitalen Zeitalter Daten oft routinemäßig erhoben und über Landesgrenzen hinweg übermittelt werden. Eine rein nationale Lösung reiche dafür nicht mehr aus. Als Vorbild für eine internationale Regelung sahen die Teilnehmer das deutsche Datenschutzrecht und wünschten sich, dass dieses einen Mindeststandard für den Schutz personenbezogener Informationen in der EU und auch darüber hinaus setzen möge. Zudem solle der neue Rechtsrahmen hinreichende Voraussetzungen für den Einsatz von Sicherheitstechnologien formulieren, einschließlich praktischer Kontroll- und Sanktionsmechanismen. Solche Mechanismen könnten auf organisatorischem Wege umgesetzt werden, wie etwa durch die Schaffung einer unabhängigen Datenschutzaufsichtsbehörde, die von jedem europäischen Bürger angerufen werden kann und die mit Einwirkungsbefugnissen gegenüber staatlichen und privaten Stellen in Europa ausgestattet ist. Um diese Behörde zu befähigen, die Privatsphäre der Bürger effektiv zu schützen, müsse diese auch adäquat mit finanziellen und personellen Mitteln ausgestattet werden. Über die organisatorischen Mittel der Kontrolle hinaus wurden technische Lösungen in den Empfehlungen durch die Forderung nach sogenannten Privacy by Design Ansätzen und mehr Forschung in der Richtung genannt. Mit solchen Lösungen, so die Erwartung der Teilnehmer, würde eine Verletzung der Privatsphäre von Anfang an nicht möglich sein. Ein

anderer Aspekt, der noch im Kontext eines umfassenden rechtlichen Rahmenwerks in Europa erwähnt wurde, ist die Stärkung des Rechts der Bürger auf Auskunft, sobald sie betroffen sind.

3.5 Wie die Bürger die Veranstaltung bewerteten

Während der und im Anschluss an die Veranstaltung gaben die Teilnehmer die Rückmeldung, dass das Bürgerforum als eine gelungene und wissensvermittelnde Veranstaltung wahrgenommen wurde. Dieser Eindruck spiegelt sich in den Antworten zu den entsprechenden Fragen wieder. Hinsichtlich des gegebenen Statements, durch die Teilnahme neue Perspektiven auf die angesprochenen Themen gewonnen zu haben, gaben 53,7 % der Teilnehmer an, dass dies eher oder gar vollständig zutreffe. 22,6 % hatten eine differenzierte Meinung hierzu, und 23,7 % sagten, dies treffe eher nicht oder überhaupt nicht zu. Eine Mehrzahl der Teilnehmer (57,8 %) meint, dass diese Veranstaltung wertvolles Wissen für die Politik erzeugt habe (siehe Tabelle unten).

			Trifft vollständig zu	Trifft eher zu	Teils, teils	Trifft eher nicht zu	Trifft überhaupt nicht zu	Keine Angabe
		N	**Prozentwerte**					
Durch die heutige Veranstaltung habe ich neue Perspektiven zu Privatsphäre und Sicherheit gewonnen.	Q106	186	29,0 %	24,7 %	22,6 %	11,3 %	12,4 %	0,0 %
Durch die heutige Veranstaltung wurde wertvolles Wissen für die Politik erzeugt.	Q107	185	36,2 %	21,6 %	27,0 %	8,1%	4.9 %	2,2 %

Tabelle 25: Wahrnehmung erlangter Erkenntnisse und erzielter Ergebnisse

Insgesamt scheinen die Bürger das Bürgerforum als eine nützliche Veranstaltung einzuschätzen, um Diskussionen anzuregen. Jedoch änderten die meisten Teilnehmer (66,5 %) trotz gewonnener Information, z. B. durch das ausgeteilte Informationsmaterial, die Kurzfilme, und die Kommunikation mit anderen in den Gruppendiskussionen nicht ihre grundlegende Haltung zu Sicherheitstechnologien. Nichtsdestotrotz gab eine Gruppe von 26,5 % an, Sicherheitstechnologien nun kritischer als zuvor zu sehen, was als eine Erhöhung des Bewusstseins um die Probleme im Hinblick auf diese Technologien durch die Veranstaltung an sich interpretiert werden kann.

Q108 – Hat die heutige Veranstaltung Ihre Einstellung zu überwachungsbasierten Sicherheitstechnologien verändert? (N= 185)

Ja, ich bin jetzt positiver eingestellt.	4,9 %
Ja, bin jetzt negativer eingestellt.	26,5 %
Nein, meine Einstellung hat sich nicht verändert.	66,5 %
Keine Angabe	2,1 %

Tabelle 26: Änderungen in der Einstellung nach dem Bürgerforum

Im Allgemeinen schätzen die Teilnehmer diese Gelegenheit, Ihre Gedanken und Meinungen mit anderen austauschen zu können. Einige äußerten sogar explizit Erleichterung, dass diese "nicht alleine mit ihrer Meinung seien", setzten sich aber auch mit unterschiedlichen Sichtweisen dahingehend auseinander, als dass diese als eine die eigene Perspektive bereichernde Erfahrung hinsichtlich der diskutierten Themen wahrgenommen würden.

4 Resümee und Schlussfolgerungen

In Deutschland haben die historischen Erfahrungen aus der Zeit des Nazi Regimes und der späteren SED-Diktatur in der früheren DDR spürbar die Sichtweise der Bürger hinsichtlich staatlicher Macht, Überwachung und Sicherheit geprägt. Die unterdrückerischen Aktivitäten der Vergangenheit haben deutliche Spuren in der deutschen Gesellschaft hinterlassen, was in einem gewissen Misstrauen gegenüber Sicherheitsinstitutionen, insbesondere Geheimdiensten, resultiert, Die Ausspähung großer Teile der deutschen Bevölkerung während dieser Zeiten der Geschichte wird noch immer so wahrgenommen, dass sie einen zerstörerischen Effekt auf den gesellschaftlichen Zusammenhalt wie auch auf die verfassungsgemäß garantierten Grundrechte des Einzelnen hat.

Bis zu einem gewissen Grad hat sich dieses Misstrauen in den letzten Dekaden verflüchtigt und ließ Raum für ein stärkeres Verlangen nach öffentlicher Sicherheit. Dies mündete in einer Prioritätenverschiebung seitens der Sicherheitsbehörden hin zu mehr präventiv orientierten Aktivitäten und Maßnahmen. Diese Veränderung der staatlichen Sicherheitspolitik wurde durch die Anschläge vom 11, September 2001 noch weiter angetrieben und führte zu einer erhöhten Akzeptanz von intensivierten Sicherheitsmaßnahmen durch die deutsche Bevölkerung. Jedoch wahrten die deutschen Bürger noch immer prinzipiell ihre kritische Haltung bezüglich Überwachung als Sicherheitslösung, während jene durch terroristische Aktivitäten wie vom 9/11 und Madrid ausgelösten Schock und Angstbefindlichkeiten teilweise allmählich nachließen. Bereits vor dem sogenannten NSA-Skandal waren die unmittelbaren wie auch die unmittelbaren, nicht sofort erkennbaren, Auswirkungen von zunehmend eingesetzten Überwachungstechnologien wiederholt Thema in der öffentlichen Diskussion von Gesellschaft, Medien und Politik. Seit den Snowden-Enthüllungen fokussiert sich eine fortdauernde öffentliche Debatte auf die Folgen globaler Überwachung, welche Grundrechte und Freiheitsrechte weltweit gefährdet. Während die Auswirkungen auf den einzelnen Bürger zunächst oft nicht sofort erkennbar sind, geraten dennoch die mittelbaren Konsequenzen für die Privatsphäre des Einzelnen und die gesellschaftlichen Folgen zunehmend in den Fokus von Medien und Politik. Riesige, unüberschaubare Datensammlungen durch Sicherheitsbehörden, oftmals ineffektive gerichtliche Kontrolle wie auch das Ungleichgewicht zwischen extensiver staatlicher Sicherheitspolitik gegenüber demokratischen Prinzipien sind hierbei die Kernthemen des wachsenden öffentlichen Diskurses.

Bei dem Bürgerforum in Deutschland wurde deutlich, dass sich die teilnehmenden Bürger durchaus sehr bewusst sind, dass Sicherheitsmaßnahmen, einschließlich überwachungsbasierter Sicherheitstechnologien, unter Umständen wichtig sein können. Nichtsdestotrotz werden ohne weiteres Einschränkungen der Privatsphäre durch solche überwachungsbasierten Sicherheitstechnologien nicht akzeptiert. Im Hinblick auf jene Technologien haben sie die Auffassung vertreten, dass diese ein erhebliches Missbrauchspotential haben, was Sorgen hinsichtlich zukünftiger Entwicklungen verstärkt. Weiterhin zweifeln die Bürger zu einem gewissen Grad die Wirksamkeit dieser Sicherheitstechnologien in Bezug auf die gewünschten Sicherheitszwecke an. Insgesamt hinterlassen die Ergebnisse der Befragung, die Gruppendiskussionen, die Tischempfehlungen und die zusätzlichen Postkarten den Eindruck, dass die Bürger eine sehr vielschichtige Sicht auf die angesprochenen Themen haben. Auf jeden Fall erkennen sie den Zweck, die Sicherheit zu erhöhen, an und berücksichtigen ihre eigenen persönlichen Erfahrungen mit Sicherheitstechnologien im Alltag wie auch die Frage, ob eine Technologie nur auf Kriminelle abzielt. Dennoch bemühten sich die Bürger, eine umfassendere Perspektive einzunehmen und die mittelbaren und langfristigen Konsequenzen von Sicherheitsmaßnahmen zu betrachten. Hierbei wurde offenbar, dass die Annahme, dass größere Risiken automatisch zu einer erhöhten Akzeptanz von überwachsungsbasierten Sicherheitstechnologien führen, falsch ist. In der Tat wurde die wahrgenommene Beeinträchtigung von Grundrechten deutlich stärker von den Teilnehmern bewertet als mögliche Vorteile der jeweils besprochenen Sicherheitstechnologie. Eine große Anzahl der teilnehmenden Bürger sagte, dass sie sich, unabhängig von wahrgenommenen Vorteilen, durch den Einsatz von Überwachungstechnologien unbehaglich und notwendigerweise nicht sicherer fühlen würden. Folglich kann nicht ohne weiteres angenommen werden, dass die Wirksamkeit einer

Sicherheitstechnologie oder die persönliche Betroffenheit alleinige Faktoren sind, die zu Akzeptanz führen. Vielmehr passt die klassische Auffassung des Sicherheit-Privatsphäre Verhältnisses nicht, welche annimmt, dass die Menschen willens seien, ihre Privatsphäre und/oder Freiheit gegen Sicherheit einzutauschen. Tatsächlich sehen die Bürger diese Sache erheblich differenzierter, wobei die Vorteile nicht automatisch die Nachteile überwiegen. Insofern gibt es ein starkes Verlangen nach einer ernsthaften Analyse der Auswirkungen von überwachungsbasierten Sicherheitstechnologien auf die betroffenen Individuen wie auch auf die Gesellschaft als Ganzes. In ihren Empfehlungen an europäische Entscheidungsträger in der Sicherheitspolitik regen die Bürger daher verschiedene Aktivitäten an, um die oben genannten Dinge zu adressieren. Mit ihren Empfehlungen fordern die Bürger:

- Weniger Überwachung allgemein um negative Auswirkungen auf die Privatsphäre zu reduzieren
- Mehr Transparenz gegenüber europäischen Bürgern
- Verpflichtende objektive Evaluation von Sicherheitstechnologien im Hinblick auf
    - Geeignetheit
    - Erforderlichkeit
    - Wirksamkeit
    - Verhältnismäßigkeit
- Ein harmonisiertes internationales (zumindest EU-weites) rechtliches Rahmenwerk, welches nicht hinter dem Schutzniveau für personenbezogene Daten gewährleistet durch das deutsche Datenschutzrecht zurückfällt
- Effektive Mittel der Kontrolle und Durchsetzung

Derzeit vermissen die Bürger eine objektive und kritische Reflexion über diese Thematik durch europäische Politiker und Sicherheitsbehörden. Es darf angenommen werden, dass dies zu den sehr deutlichen Ergebnissen hinsichtlich der Vertrauenswürdigkeit von Sicherheitsinstitutionen geführt hat. Diese zeigen klar, dass die Bürger die derzeitigen Schwerpunkte der Sicherheitspolitik in Deutschland als zu eindimensional und unreflektiert im Hinblick auf individuelle wie auch gesellschaftliche Folgen von Überwachung ansehen. Während der Veranstaltung stützten und bezogen sich die Bürger oftmals auf die historischen Erfahrungen der deutschen Bevölkerung, um Beispiele dafür anzubringen, wie staatliche Sicherheitspolitik zu einer Ausweitung der Zweckbestimmung und zu Missbrauch der Macht des Staates gegen die eigenen Bürger führen kann. Daher kann angenommen werden, dass den staatlichen Institutionen, desto mehr Vertrauen ihnen entgegengebracht wird, umso besser die Kontrollmechanismen sind – entsprechend steigt auch die Akzeptanz bezüglich der Nutzung von Sicherheitstechnologien. Jedoch ist gerade die Frage der Akzeptanz eine sehr vielschichtig betrachtete, wobei die Bürger eine vorsichtige Balance zwischen den Vorteilen einer Technologie gegenüber den zu erwartenden Beeinträchtigungen ihrer Privatsphäre haben. In diesem Sinne sind die Bürger nicht bereit, bedingungslos weder ihre individuelle Privatsphäre noch die Privatheit als allumfassendes gesellschaftliches Konzept gegen Verbesserungen der öffentlichen Sicherheit einzutauschen. Vielmehr kritisierten sie das sogenannte "Trade-off" Modell als zu simpel und verlangten eine ausgewogene Balance zwischen Privatsphäre und Sicherheit. Dies schließt eine ernsthafte Evaluation und fortdauernde kritische Überprüfung von Geeignetheit, Adäquanz und Verhältnismäßigkeit von überwachungsbasierten Sicherheitstechnologien mit ein, einhergehend mit hinreichender Transparenz und Kontrolle der anwendenden Sicherheitsinstitutionen.

5 Quellenverzeichnis

Alvares de Souza Soares, Philip, Spiegel Online, 5, März 2014, "Amtliche Spähsoftware: Staatstrojaner-Fiasko verbittert Polizisten": http://www.spiegel.de/netzwelt/netzpolitik/warum-es-bis-heute-keinen-staatstrojaner-gibt-a-956617.html

Arbeitskreis Vorratsdatenspeicherung, Webseiteninformation über die Beschwerde vor dem Bundesverfassungsgericht gegen die deutsche Umsetzung der EU Richtlinie zur Vorratsdatenspeicherung: http://www.vorratsdatenspeicherung.de/content/view/51/1/lang.de/ %3E

Beckedahl, Markus, Netzpolitik,org, 7, Februar 2012, “Zwischenstand: 12 Millionen Funkzellenabfragen in Berlin”: https://netzpolitik.org/2012/zwischenstand-12-millionen-funkzellenabfragen-in-berlin/

Berliner Verwaltungsgericht

- Entscheidung vom 5. Juli 2010, (Az, 1 K 905,09): http://www.gerichtsentscheidungen.berlin-brandenburg.de/jportal/?quelle=jlink&docid=JURE100068408&psml=sammlung.psml&max=true&bs=10
- Entscheidung vom 26. April 2012 (Az, Az, VG 1 K 818,09): www.gerichtsentscheidungen.berlin-brandenburg.de/jportal/?quelle=jlink&docid=JURE120017238&psml=sammlung,psml&max=true&bs=10

Berliner Beauftragter für den Datenschutz und die Informationsfreiheit, Bericht vom 3. September 2012, „Abschlussbericht zur rechtlichen Überprüfung von Funkzellenabfragen“: http://www.datenschutz-berlin.de/attachments/896/Pr__fbericht.pdf?1346753690

Biermann, Kai, Zeit Online Artikel vom 26, März 2006, "Betrayed by our own data": http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz

Brinkmann, Bastian; Hollenstein, Oliver; Kempmann, Antonius, Sueddeutsche.de, 16. November 2013, "Was Spionagefirmen in Deutschland für die USA treiben": http://www.sueddeutsche.de/politik/amerikanische-auftragnehmer-was-spionagefirmen-in-deutschland-fuer-die-usa-treiben-1.1820034

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI), Tätigkeitsbericht für die Jahre 2011-2012: http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/24TB_2011_2012.pdf?__blob=publicationFile

Bundesministerium der Justiz, Webseiteneintrag vom 10. Juni 2011, "Quick-Freeze: Bundesjustizministerin legt Gesetzentwurf vor": http://www.bmj.de/DE/Service/Newsletterversand/_doc/_inhalt/092011_001.html

Deutscher Bundestag, Drucksache 17/14600 vom 22. August 2013, "Beschlussempfehlung und Bericht des 2, Untersuchungsausschuss es nach Artikel 44 des Grundgesetzes" (PDF-file): http://dipbt.bundestag.de/dip21/btd/17/146/1714600.pdf

Deutsches Bundesverfassungsgericht

- Entscheidung vom 15, Dezember 1983 (Az,: 1 BvR 209, 269, 362, 420, 440, 484/83): https://openjur.de/u/268440.html
- Entscheidung vom 3. März 2004, (Az,: 1 BvR 2378/98): http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.htmlDecision of 27th February 2008, (Az,: 1 BvR 370/07): http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html
- Entscheidung vom 11. März 2008, (Az,: 1 BvR 256/07): http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr025608.html
- Entscheidung vom 24. April 2013, (Az,: 1 BvR 1215/07): https://www.bundesverfassungsgericht.de/entscheidungen/rs20130424_1bvr121507.html

Deutsches Bundesverwaltungsgericht, Entscheidung vom 25. Januar 2012, (Az, BVerwG 6 C 9,11): http://www.bverwg.de/enid/069768c9c3aa31f1baef81da1db91409,54e4b07365617263685f646973706c6179436f6e7461696e6572092d093134303632093a095f7472636964092d093133333430/Pressemitteilungen/Pressemitteilung_9d.html

Deutscher Städte- und Gemeindebund (DStGB) und Gewerkschaft der Polizei (GdP), Veröffentlichung vom 27. Januar 2014: " Sicherheit in Städten und Gemeinden – Positionspapier des Deutschen Städte- und Gemeindebundes (DStGB) und der Gewerkschaft der Polizei (GdP)"

Deutsche Wikipedia, Eintrag zum NSA Skandal; Untertitel "Basisdemokratische Initiativen" : http://de.wikipedia.org/wiki/Globale_ %C3 %9Cberwachungs-_und_Spionageaff %C3 %A4re#Basisdemokratische_Initiativen

Die Welt, 13. November 2011 "Friedrich spricht erstmals von "Rechtsterrorismus": http://www.welt.de/politik/deutschland/article13714953/Friedrich-spricht-erstmals-von-Rechtsterrorismus.html

Die Welt, 22, Juni 2011, "EU leitet Verfahren gegen Deutschland ein": http://www.welt.de/politik/deutschland/article13443492/EU-leitet-Verfahren-gegen-Deutschland-ein.html

Ehrenberg, Markus, Der Tagesspiegel Artikel vom 18. Juli 2012, “Sinnvoll skandalös”: http://www.tagesspiegel.de/medien/datenschutz-sinnvoll-skandaloes/6888806.html

European Digital Rights, EDRI Webseiteneintrag über die verstärkte Nutzung stiller SMS zur Aufspürung Verdächtiger durch die deutsche Polizei: http://www.edri.org/edrigram/number10.2/silent-sms-tracking-suspects

Europäischer Gerichtshof der Europäischen Union, Entscheidung in den verbundenen Verfahren C-293/12 und C-594/12Digital Rights Ireland, Seitlinger und andere:

http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

Fuchs, Christian; Goetz, John; Obermaier, Frederik, in Sueddeutsche.de, Artikel vom 13. September 2013, "Verfassungsschutz beliefert NSA": https://web.archive.org/web/20131003031334/http://www.sueddeutsche.de/politik/spionage-in-deutschland-verfassungsschutz-beliefert-nsa-1.1770672

Heise online, 25. Februar 2012, “Geheimdienste überwachten 37 Millionen Netzverbindungen“: http://www.heise,de/newsticker/meldung/Geheimdienste-ueberwachten-37-Millionen-Netzverbindungen-1442867.html

Hunton & Williams LLP,, Privacy and Information Security Law Blog, Eintrag vom 7. Juli 2011, “Germany Launches National Cyber Defense Center”: http://www.huntonprivacyblog.com/2011/07/articles/germany-launches-national-cyber-defense-center/

Meiritz, Annett; Musharbash, Yassin; Weiland, Severin, in: Spiegel Online vom 21. November 2011, "Ermittlungspannen bei Neonazi-Mordserie: die Schuld der Behörden": http://www.spiegel.de/politik/deutschland/ermittlungspannen-bei-neonazi-mordserie-die-schuld-der-behoerden-a-799074.html

Mitteldeutsche Zeitung, 3. August 2013, "Bundesanwaltschaft prüft Ermittlungen zur NSA-Affäre": http://www.mz-web.de/politik/bundesanwaltschaft-prueft-ermittlungen-zur-nsa-affaere.20642162.23903482.html

Müller, Thorsten, Bundeszentrale für politische Bildung, 14. Juni 2012, "Innere Sicherheit in der Europäischen Union": http://www.bpb.de/politik/innenpolitik/innere-sicherheit/76658/europaeisierung-von-innerer-sicherheit

Neumann, Linus, Netzpolitik,org, 20. Juni 2011, "Dresden: Demoüberwachung mittels Mobilfunknetz": https://netzpolitik.org/2011/dresden-demouberwachung-mittels-mobilfunknetz/

rbb-Kultursendung “Stilbruch” vom 15. August 2013, betitelt "Freiheit im Internet": http://www.rbb-online.de/stilbruch/archiv/20130815_2215/freiheit-im-internet.html

Sächsischer Datenschutzbeauftragter, Bericht über nichtindividualisierte Funkzellenabfragen und andere Maßnahmen der Telekommunikationsüberwachung durch Polizei und Staatsanwaltschaft in Dresden im Februar 2011: http://www.saechsdsb.de/images/stories/sdb_inhalt/behoerde/oea/bericht-funkzellenabfragen.pdf

Scholz, Alexander, Searchlight Magazin Blog Artikel vom 7. Juli 2012, “Germany to tackle neo-Nazis with database”: http://www.searchlightmagazine.com/news/international-news/germany-to-tackle-neo-nazis-with-database

Spiegel Online, 10. Mai 1971, "EDV im Odenwald": http://www.spiegel.de/spiegel/print/d-43176393.html

Spiegel Online, 4. September 2006, “Innenminister-Konferenz: Zweiteilige Anti-Terror-Datei kommt”: http://www.spiegel.de/politik/deutschland/innenminister-konferenz-zweiteilige-anti-terror-datei-kommt-a-435082.html

Spiegel Online, 31. August 2011, „Flugsicherheit: Nacktscanner versagen im Praxistest“: http://www.spiegel.de/reise/aktuell/flugsicherheit-nacktscanner-versagen-im-praxistest-a-783550.html

Spiegel Online, 3. August 2013, "Überwachung: BND leitet massenhaft Metadaten an die NSA weiter":
http://www.spiegel.de/netzwelt/netzpolitik/bnd-leitet-laut-spiegel-massenhaft-metadaten-an-die-nsa-weiter-a-914682.html

Tagesschau, Bericht vom 7. August 2013, "BND-NSA-Kooperation: Streit über Steinmeiers Rolle":
https://web.archive.org/web/20131004220036/http://www.tagesschau.de/inland/bndnsa102.html

The H Security Blog, Artikel vom 10. Oktober 2011, “CCC cracks government Trojan”:
http://www.h-online.com/security/news/item/CCC-cracks-government-trojan-1357755.html

The H Security Blog, Artikel vom 26. Oktober 2011, “CCC criticizes new version of government Trojan”:
http://www.h-online,com/security/news/item/CCC-criticises-new-version-of-government-trojan-1367160.html

The H Security Blog, Artikel vom 11. September 2012, “Federal Commissioner unable to audit Federal Trojan source”:
http://www.h-online,com/security/news/item/Federal-Commissioner-unable-to-audit-Federal-Trojan-source-1704460.html

Vensky, Hellmuth, Zeit Online, 9. Juli 2012, “Die Fallstricke der Facebook-Fahndung”:
http://www.zeit.de/digital/datenschutz/2012-07/facebook-fahndung-hessen

Zeit Online, 14. Januar 2014, " De Maizière sieht Deutschland gleich mehrfach bedroht":
http://www.zeit.de/politik/deutschland/2014-01/de-maiziere-gefahren-terrorismus

Zeit Online, 28. Februar 2014, "Steinmeier rückt von Anti-Spionage- Abkommen ab":
http://www.zeit.de/politik/ausland/2014-02/usa-kein-no-spy-abkommen

6 Abbildungsverzeichnis

7 Tabellenverzeichnis

8 Abkürzungsverzeichnis

Abkürzung	Definition
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BND	Bundesnachrichtendienst
CCC	Chaos Computer Club
DDR	Deutsche Demokratische Republik
CCTV	Closed circuit television
GdP	Gewerkschaft der Polizei
EC	European Commission
EU	European Union
NSA	National Security Agency
PbD	Privacy by Design
Stasi	Staatssicherheitsdienst