Deutscher Bundestag
1. Untersuchungsausschuss
der 18. Wahlperiode

MAT A SV-6

zu A-Drs.: 69

Untersuchungsausschuss des Deutschen Bundestags
Sachverständigengutachten
Ben Scott
15. Juli 2015

Inhaltsverzeichnis

Einleitung

Die Offenlegung von NSA-Dokumenten durch Edward Snowden im Juni 2013 führte zu einer hitzigen Debatte über Menschenrechte und bürgerliche Freiheiten im digitalen Zeitalter – nicht nur in Berlin und Brüssel, sondern auch in Washington. Führungspersönlichkeiten aus Politik, Wirtschaft und der Zivilgesellschaft weltweit riefen zu schnellen Änderungen von Gesetzen und Politik auf, um diese Probleme sowohl in den USA als auch in ihren Heimatländern zu lösen. Aber zwei Jahre später haben in keinem Land umfangreiche Änderungen von Gesetzen und Politik stattgefunden – obwohl sehr viel mehr darüber bekannt ist, durch wen und wie welche Überwachung erfolgt. Deutschland ist die einzige Nation, die noch öffentlich fordert, dass die USA und das Vereinigte Königreich ihre Methoden ändern. Kein Land hat den Versuch unternommen, mit einem Beispiel bei den Reformanstrengungen voranzugehen. Die meisten Länder haben eine stillschweigende Anpassung vorgenommen. Andere beantworten Sicherheitsbedrohungen eher mit einer Liberalisierung als mit einer Verschärfung des Überwachungsrechts.[1]

Die Geschichte ist jedoch nicht abgeklungen. Die Schlagzeilen gehen weiter und dokumentieren mit bekannt gewordenen geheimen Unterlagen die Einzelheiten der Reichweite der NSA innerhalb der Kommunikationsnetze von Freunden wie von Feinden. Inzwischen haben die von Deutschland angeführten Untersuchungen dieser Angelegenheiten – einschließlich der von diesem Ausschuss betriebenen Untersuchung – in erster Linie neue Informationen über die Komplizenschaft des BND an der digitalen Überwachung geliefert, und weniger neue Erkenntnisse über die NSA. Zwei Jahre nach Snowden geht es nicht nur um die Macht der amerikanischen Signalaufklärung, sondern es handelt sich um ein komplexes Thema mit ineinandergreifenden Behörden, kooperativen Überwachungsoperationen, asymmetrischem Informationsaustausch und großen Lücken zwischen dem, was Sicherheitsbehörden tun, und dem, was gewählte Amtsträger (und die Öffentlichkeit) darüber wissen. Die jüngsten Behauptungen lassen jetzt vermuten, dass die Ziellisten der NSA innerhalb der deutschen Regierung bei weitem nicht nur die Kanzlerin betrafen.[2] Aber ebenso wird auch der BND beschuldigt, das Abfangen von Kommunikationen zwischen benachbarten europäischen Staaten zu ermöglichen oder aktiv zu betreiben.[3] Und es gibt kaum Zweifel daran, dass die Zusammenarbeit zwischen BND und NSA umfangreich ist.[4]

Die Erfahrung der letzten zwei Jahre führt für viele zu einem beunruhigenden Schluss: Selbst der nie dagewesene Umfang und politische Schock der Snowden-Offenlegungen bewirkt in demokratischen Staaten keine schnelle und energische Reform der Politik in Bezug auf Sicherheit und Privatsphäre. Deswegen kommt man leicht zu dem zynischen Schluss, dass sich nichts ändern wird und die Störung des Vertrauens zwischen Verbündeten bestehen bleibt. Auf längere Sicht gibt es aber Anlass zu Optimismus.

---

[1] Martin Untersinger, “If You Can’t Beat ’Em: France, Up In Arms Over NSA Spying, Passes New Surveillance Law”, *The Intercept*, 24. Juni 2015, https://firstlook.org/theintercept/2015/06/24/france- protests-nsa-spying-passes-new-surveillance-law/

[2] Georg Mascolo, et al., “Von Kohl bis Merkel - die NSA hörte mit”, *Süddeutsche.de*, 8. Juli 2015, http://www.sueddeutsche.de/politik/wikileaks-dokumente-von-kohl-bis-merkel-die-nsa-hoerte-mit- 1.2556461

[3] Gerald Traufetter, “BND-Affäre: Österreichischer Abgeordneter zeigt Telekom und BND an”, *Spiegel.de*, 18. Mai 2015, http://www.spiegel.de/netzwelt/netzpolitik/bnd-affaere-oesterreichischer-abgeordneter- zeigt-telekom-und-bnd-an-a-1034297.html

[4] Georg Mascolo, “Codewort Eikonal - der Albtraum der Bundesregierung”,*Sueddeutsche.de*, 4. Oktober 2014, http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der- bundesregierung-1.2157432

Wie diese Stellungnahme zeigen wird, ist in den USA eine lange und hitzige Reformdebatte im Gange, und es wurden erhebliche Fortschritte bei einer langen Liste politischer Veränderungen erzielt. Das Kernproblem für Europäer wurde dabei nicht gelöst – ob und wie die NSA die Überwachung ausländischer Bürger einschränken wird. Die direkte Antwort ist, dass sie das nicht tun wird, obwohl mit den Reformen die Transparenz stark verbessert wurde und Nicht-US-Personen höhere Standards für Privatsphäre und bürgerliche Freiheiten gewährt wurden.[5] Trotzdem sind die politischen Veränderungen in Washington nicht nur rechtlich bedeutsam. Sie sind bedeutsam, weil sie einen Wandel in der Art anzeigen, wie die amerikanische Öffentlichkeit und die US-Regierung die Notwendigkeit und die Legitimität von Überwachung verstehen. Das ist ein Anfang – eine klare Grundlinie in einem Rechtsbereich, der lange geheim war – für ein langes Engagement für eine demokratische Gesellschaft, die die politische Behandlung von Privatsphäre und Sicherheit im digitalen Zeitalter modernisieren möchte.

Man sollte die folgende Erklärung von Präsident Barack Obama von Dezember 2013 beachten:

> *„Ich denke, was bei dieser ganzen Übung auch wichtig war, ist die Erkenntnis, dass in einer virtuellen Welt diese Grenzen teilweise keine Rolle mehr spielen. Und dass wir etwas tun können, heißt nicht, dass wir es unbedingt tun sollten, und die Werte, die wir als Amerikaner erlangt haben, müssen wir auch jenseits unserer Grenzen anzuwenden bereit sein, und zwar, denke ich, vielleicht systematischer als in der Vergangenheit.“*[6]

Im Zentrum von Präsident Obamas Kommentar liegt die Spannung zwischen dem Legalen (und technisch Möglichen) einerseits und dem Legitimen andererseits. Was legal ist, ist nicht unbedingt auch legitim. Deswegen greifen wir oftmals Debatten über Gesetze wieder auf, insbesondere dann, wenn sie kontrovers sind. Kontext, Interpretation und Umsetzungsmethoden spielen eine große Rolle in der Festlegung der öffentlichen Legitimität. Im Kern geht es in der Debatte über NSA-Praktiken im Grunde um die Umstände, unter denen Überwachung in einer Demokratie legitim ist. In keinem Land wurde ernsthaft der Vorschlag gemacht, Überwachung jeglicher Art illegal zu machen. Und es wurde nicht ernsthaft vorgeschlagen, alle Arten von „Massenüberwachung“ abzuschaffen. Aber viele Länder – vielleicht bemerkenswerterweise vor allem die USA und Deutschland – debattieren darüber, was legitim ist. Und in bestem demokratischem Geist ist es das Ziel, das Gesetz so zu modernisieren, dass es dem Urteil entspricht, zu dem wir gelangen.

Diese Frage der Legitimität sollte die zentrale Linse sein, durch die dieser Ausschuss die Aktionen seiner eigenen Regierung ebenso wie diejenigen anderer Nationen sieht. Legitimität bedeutet drei Dinge. Erstens ist es das Vertrauen darauf, dass die Macht transparent und in einem ordnungsgemäßen Verfahren gemäß dem Gesetz angewandt wird. Zweitens ist Legitimität das Vertrauen darauf, dass die Macht durch demokratische Prinzipien eingeschränkt wird. Und drittens ist Legitimität mit der effektiven Beaufsichtigung und Rechenschaftspflicht über die Anwendung der Macht mit klaren und effektiven Kontrollen verbunden. Selbst in einer Nach-Snowden-Welt ist die Mehrheit in Europa und in den USA nicht gegen digitale Überwachung zur Durchsetzung von Gesetzen und zur Aufklärung. Was sie möchte,

---

[5] Im Folgenden wird „US-Personen“ als Begriff des US-Rechts benutzt und bedeutet US-Bürger oder Personen mit rechtmäßigem dauerhaftem Wohnsitz in den USA. Siehe z. B. https://www.nsa.gov/about/faqs/oversight.shtml#oversight3

[6] Edward Moyer, “Obama: NSA programs could be ‘redesigned’ to prevent abuses”, *cnet.com*, 20. Dezember 2013, http://www.cnet.com/news/obama-nsa-programs-could-be-redesigned-to-prevent- abuses/

sind stärkere Garantien dafür, dass die Anwendung der staatlichen Macht klar und begrenzt ist und innerhalb der Nationen sowie zwischen ihnen ordnungsgemäß kontrolliert wird.

Ich wurde vom Ausschuss gebeten, einen Überblick der Nach-Snowden-Debatte und der Reformanstrengungen in den USA zu geben. Eine sorgfältige Dokumentation von Argumenten, Gegenargumenten, Studien, Berichten und (vorgeschlagenen und verabschiedeten) Politikänderungen würde leicht ein Buch füllen. Und ein beträchtlicher Teil davon würde von Amerikanern handeln, die darüber debattieren, wie und ob die NSA deren eigene Persönlichkeitsrechte beachtet – ohne Bezug zu den internationalen Fragen, mit denen dieser Ausschuss befasst ist. Nach sorgfältiger Abwägung der Frage, was für die Arbeit dieses Ausschusses am besten geeignet sein könnte, bin ich zu dem Schluss gekommen, dass ich meine Stellungnahme auf die Frage konzentrieren sollte, die für die Deutschen am wichtigsten ist. Zwar ist die Debatte über die Auswirkungen der Überwachungsprogramme auf Amerikaner wichtig und bedeutend, aber die Deutschen interessieren sich natürlich am meisten für die Auswirkungen dieser Programme auf ihre eigene Privatsphäre.

Diese Frage geht direkt zum Kern des Problems der Legitimität. Wenn es um die Tätigkeit seiner Auslandsnachrichtendienste geht, zieht jedes demokratische Land eine Trennungslinie zwischen Bürgern und Personen, die in seinem Hoheitsgebiet wohnen (im US-Kontext als US-Personen bezeichnet) und allen anderen Personen. Aus deutscher Sicht bedeutet das, dass Deutsche gegenüber der von deutschen Regierungsstellen vorgenommenen Überwachung bestimmte Rechte und Schutzvorkehrungen genießen. Was aber die von NSA, GCHQ oder anderen Stellen vorgenommene Überwachung betrifft, sind die Deutschen sehr viel mehr Freiwild. Während die russische und die chinesische Regierung sich möglicherweise nicht um diese Diskriminierung bei den Persönlichkeitsrechten kümmern (da sie sie möglicherweise noch nicht einmal ihren eigenen Bürgern gewähren), stellt dies für jede liberale Demokratie ein Legitimitätsproblem dar. Wie Präsident Obama sagte: „dass wir etwas tun *können*, heißt nicht, dass wir es unbedingt tun *sollten.*“ (Hervorhebung hinzugefügt)

Im Kontext internationaler Beziehungen und der Überwachungspolitik ist die Schlüsselfrage, wie die nationalen Gesetze, die die Sammlung nachrichtendienstlicher Informationen regeln, mit den Persönlichkeitsrechten und den bürgerlichen Freiheiten von Ausländern umgehen – das „Diskriminierungsproblem“. Die Behandlung des Diskriminierungsproblems wird in jeder Nation für die Entwicklung eines gesetzlichen Rahmens für die Sammlung auslandsnachrichtendienstlicher Informationen, der nicht nur von ihren eigenen Bürgern, sondern auch von den Verbündeten und Partnern dieses Landes als legitim angesehen wird, ein zentrales Element sein. Das Diskriminierungsproblem ist in den USA klar als zentrales Element erkannt worden. Es ist keine Überraschung, dass die Menschenrechtsorganisationen den Mangel an Schutzmechanismen für die Privatsphäre von Nicht-US-Personen stark kritisieren. Sie argumentieren, dass das eine klare Verletzung der im Rahmen der Menschenrechtsverträge bestehenden Verpflichtungen ist. Die deutsche und die brasilianische Regierung haben der UNO-Generalversammlung eine gemeinsame Resolution vorgelegt, in der auf die Menschenrechtsverletzungen aufmerksam gemacht wird, die sich aus der extraterritorialen Massenüberwachung ergeben können.[7]

Inzwischen gehören Technologie- und Internetunternehmen aus den USA zu den Befürwortern von Reformen, mit denen ausländischen Bürgern mehr Schutz gewährt wird. Diese Unternehmen handeln nicht uneigennützig. Als globale Unternehmen sind sie in erster Linie über den Verlust von Marktanteilen

[7] Deutsche Welle, “Germany and Brazil circulate UN draft resolution on condemning surveillance”, 2. November 2013, http://www.dw.com/en/germany-and-brazil-circulate-un-draft-resolution-on-condemning- surveillance/a-17199877

in Übersee besorgt. Beispielsweise reagierte der CEO von Facebook, Mark Zuckerberg, entrüstet auf die erste Antwort der US-Regierung hinsichtlich des Prism-Programms.

> *Die Antwort der Regierung war: ‚Kein Grund zur Sorge, wir spionieren keine Amerikaner aus.' Das ist doch wunderbar; es ist sehr hilfreich für Unternehmen, die Menschen auf der ganzen Welt bedienen, und es wird das Vertrauen in amerikanische Internetunternehmen stärken.*[8]

Nach zweijähriger Debatte ist Silicon Valley zu einem mächtigen Verbündeten derjenigen geworden, die nicht nur die Persönlichkeitsrechte von US-Bürgern, sondern aller Menschen weltweit verbessern wollen. Diesen Unternehmen ist es zwar nicht gelungen, die Politiker dazu zu bewegen, eine allgemeingültige Norm für Persönlichkeitsrechte zu verabschieden, aber sie haben eine neue Genehmigung erwirkt, ihre eigene Transparenz bezüglich der Art und der Häufigkeit von Datenanforderungen, die von Strafverfolgungsbehörden an sie gerichtet werden, zu erhöhen.

Nach vielen Debatten, Überprüfungen und Beratungen hat die US-Regierung mehrere Reformen auf dem Gebiet der Persönlichkeitsrechte von Nicht-US-Personen verabschiedet. In den europäischen Medien fanden diese Reformen wenig Beachtung. Aber sie zeigen, dass es dauerhafte Bemühungen gibt, auf die Bedenken ausländischer Regierungen und Bürger einzugehen, die Transparenz hinsichtlich der Grundsätze, Umstände und Verfahren der Sammlung auslandsnachrichtendienstlicher Erkenntnisse zu erhöhen und konkrete Änderungen am Gesetz und in der Praxis vorzunehmen. Diese Bemühungen reichen bei weitem nicht aus, um das Diskriminierungsproblem zu lösen. Aber sie sind ein wichtiger Ausgangspunkt für künftige Reformen. Und ich argumentiere damit, dass jedes Land, das die US-Regierung bezüglich des Diskriminierungsproblems in die Pflicht nehmen will, zumindest die Schwelle dieser Reformen erfüllen muss. Wie ich in meinem Fazit zeigen werde, hat Deutschland mit der Arbeit dieses Ausschusses und der Intensität und Ernsthaftigkeit der Debatte in Berlin eine starke Position erlangt, um eine sehr viel höhere Norm festzulegen. Wie aber der Fall USA zeigt, ist dazu ernsthafte Arbeit erforderlich.

Mein konkretes Ziel in dieser Stellungnahme ist es, kurz die politische Debatte über die Überwachung in den USA in der Nach-Snowden-Zeit zu beschreiben und die politischen Reformen zu bewerten, die vorgeschlagen oder verabschiedet wurden – besonders diejenigen, die von Bedeutung sind für die Persönlichkeitsrechte und bürgerlichen Freiheiten von Nicht-US-Personen. Im ersten Abschnitt zeige ich, wie das US-Recht für die Beaufsichtigung und Leitung der Praxis der Signalaufklärung strukturiert ist. Im zweiten Abschnitt bespreche ich die wichtigsten Reformanstrengungen, die von der Regierung Obama begonnen und/oder zu Ende geführt wurden. Im dritten Abschnitt schließlich möchte ich auf die Themen dieser Einleitung zurückkommen und zum Ausdruck bringen, dass die Reformdebatte der letzten zwei Jahre in den USA als ein Anfang aufgefasst werden sollte und nicht als ein Ende. Wie aber die Arbeit dieses Ausschusses gezeigt hat, wird und kann das Überwachungsproblem nicht in Washington allein gelöst werden. Die von der Regierung Obama verabschiedeten Reformen legen eine neue Grundlinie von Rechten, Normen und Transparenz in den Überwachungspraktiken demokratischer Gesellschaften fest. Sie bleibt womöglich deutlich hinter den Wünschen und Erwartungen der europäischen Verbündeten Amerikas zurück. Aber sie stellt eine Arbeitsgrundlage dar – die Verfahrensweisen wurden aus der geheimen Welt der Geheimdienstbehörden herausgenommen und für Untersuchung und Debatte öffentlich gemacht.

---

[8] Dominic Rushe, "Zuckerberg: US government 'blew it' on NSA surveillance", *TheGuardian.com*, 12. September 2013, http://www.theguardian.com/technology/2013/sep/11/vahoo-ceo-maver-iail-nsa- surveillance

Deutschland kann mit seinen historischen Verpflichtungen im Hinblick auf Privatsphäre und bürgerliche Freiheiten mit gutem Beispiel vorangehen, Argumente für weitere Reformen vorbringen und neue Gesetzes- und Legitimitätsnormen setzen, denen alle anderen Nationen folgen können und vor deren Hintergrund alle anderen Nationen beurteilt werden.

Teil 1: Übersicht der US-Überwachungsbestimmungen

Der Gesetzesrahmen für die Überwachung zu nachrichtendienstlichen Zwecken (im Unterschied zur öffentlichen Überwachung und zur Strafverfolgung) enthält drei Grundelemente – Genehmigung, Durchführung und Beaufsichtigung. Die erste Gruppe von Vorschriften regelt die Grundsätze, Normen und Prozesse für die Genehmigung einer Überwachungsaktion. Die zweite Gruppe von Vorschriften gilt für Überwachungsaktionen, die genehmigt wurden. Sie betrifft Einschränkungen wie die Dauer der Überwachung, den Zeitraum der Datenspeicherung, die unbeabsichtigte Erfassung, Fehler oder Falschmeldungen und Vorschriften zum Datenaustausch mit anderen Behörden. In der dritten Gruppe von Vorschriften schließlich ist die Beaufsichtigungspraxis innerhalb der Geheimdienstbehörde, innerhalb der Exekutive der Regierung, der die Geheimdienstbehörde unterstellt ist, und innerhalb der zur Führung der Regierung gewählten Legislative festgelegt. Reichweite und Auftrag der Beaufsichtigungsinstrumente sind entscheidend dafür, ob es ausreicht, die Entscheidungsträger bezüglich der Normen für die Genehmigung und für die Durchführung zur Rechenschaft zu ziehen.

In den USA unterliegt die Sammlung auslandsnachrichtendienstlicher Erkenntnisse diesen drei Bereichen im Rahmen verschiedener Gesetze und Durchführungsverordnungen/Richtlinien, die je nach dem Ziel und der Art der Überwachung in unterschiedlicher Weise angewandt werden. Eine vollständige Analyse aller Variationen, wie bestimmte Gesetze bestimmte Arten von Überwachungsaktionen regeln, geht über den Rahmen dieser Stellungnahme hinaus und ist für ihre Zwecke überflüssig. Eine kurze Diskussion der drei häufigsten Gesetzesgrundlagen reicht aus, um die Hauptpunkte aufzuzeigen.[9]

Section 215 des PATRIOT Act (2001)[10]: Dieses Gesetz wurde auf die Terroranschläge vom 11. September hin erlassen. Diese Vorschrift erlaubt die Erfassung von „greifbaren Dingen“ oder „Geschäftsunterlagen“ zur Unterstützung von Ermittlungen mit auslandsnachrichtendienstlichem Zweck – beispielsweise Terrorismusbekämpfung. Insbesondere wurde dieses Gesetz benutzt, um die Massenerfassung von Metadaten aller von Einwohnern der USA ausgehenden oder bei ihnen ankommenden Telefonanrufe durch die NSA zu genehmigen. Zielpersonen im Rahmen dieses Gesetzes sind Nicht-US-Personen, bei denen vernünftige Gründe für die Annahme bestehen, dass die aufgezeichneten persönlichen Daten auslandsnachrichtendienstliche Erkenntnisse enthalten, die für Ermittlungen von Bedeutung sind. Mit Section-215-Anordnungen kann eine sehr breite Erfassung von Daten genehmigt werden. Sie werden von dem Foreign Intelligence Surveillance Court (FISC) genehmigt. Aktionen, die mit diesen Datensätzen durchgeführt werden, sind durch Nutzungs- und Minimierungspraktiken eingeschränkt. Dabei handelt es sich entweder um standardisierte Praktiken

[9] Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies, “Liberty and Security in a Changing World”, 12. Dezember 2013, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12 rg final report.pdf (siehe Anhang A) ; Ian Brown et al., “Towards Multilateral Standards for Surveillance Reform”, http://voxpol.eu/wp-content/uploads/2015/01/HERE.pdf

[10] H.R. 3162, “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001”, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107 cong bills&docid=f:h3162enr.txt.pdf

innerhalb der NSA oder des FBI, oder sie werden vom FISC spezifiziert.[11] Die Beaufsichtigung der Section-215-Programme erfolgt durch die durchführenden Behörden selbst, den Director of National Intelligence, das Justizministerium sowie den Privacy and Civil Liberties Oversight Board und die Geheimdienstausschüsse des Kongresses.

Foreign Intelligence Surveillance Act (1978)[12]: Der FISA wurde nach den Watergate-Skandalen der Nixon-Ära, bei denen Bundesbehörden zum Ausspionieren amerikanischer Bürger benutzt wurden, verabschiedet. Mit dem FISA wurden neue Vorschriften für Überwachungsaktivitäten zum Zwecke der Sammlung auslandsnachrichtendienstlicher Erkenntnisse und ihrer Beaufsichtigung erlassen, wobei ausdrücklich zwischen den für US-Personen und für Nicht-US-Personen geltenden Normen unterschieden wurde. Mit dem FISA wurde das Foreign Intelligence Surveillance Court (FISC) eingerichtet, das geheime Anträge von Behörden zur Durchführung von Überwachungsaktionen für bestimmte Zwecke, beispielsweise Terrorismusbekämpfung, überprüft.

Der FISA wurde im Laufe der Jahre oft geändert, insbesondere durch den FISA Amendments Act von 2008 (FAA). Der FAA enthielt eine neue Bestimmung – Section 702 –, mit der Auslandsüberwachungsaktionen, die Nicht-US-Personen außerhalb der USA zum Ziel haben, zur Erfassung von Telekommunikationsdaten (einschließlich Telefonats- und E-Mail-Inhalten) durch die NSA konkret erlaubt wurden. Der Justizminister und der Director of National Intelligence können Nicht-US-Personen für Zeiträume von bis zu einem Jahr als Zielpersonen festlegen. Eine spezielle richterliche Prüfung für bestimmte Zielpersonen war nicht erforderlich, wenn die Zielperson einer vom FISC genehmigten breiten Zertifizierung für die Erfassung auslandsnachrichtendienstlicher Erkenntnisse unterliegt. Diese jährlichen Genehmigungen müssen vom FISC gebilligt werden, und sie werden dem (geheimen) National Intelligence Priorities Framework entnommen. Die umfangreichen Leitlinien für Einschränkungen von Section-702-Operationen (Minimierungspraktiken) wurden freigegeben und veröffentlicht.[13] Sie enthalten spezifische Anweisungen für die Behandlung, Speicherung, Abfrage und Verarbeitung der Daten. Die Section-702-Operationen werden von der NSA selbst, dem DNI und den Aufsichtsausschüssen des Kongresses überwacht.

Mit Section 702 des Foreign Intelligence Surveillance Act werden zwei bekannte Massenerfassungsprogramme genehmigt, die durch die Snowden Files enthüllt wurden: PRISM und UPSTREAM.[14] Das PRISM-Programm schreibt vor, dass teilnehmende US-Internetunternehmen Kommunikationen übergeben, die mit Selektoren (E-Mail-Adresse, Kontenname usw.), die sie von einer Sicherheitsbehörde erhalten, zusammenhängen. Das UPSTREAM-Programm ist sehr viel breiter angelegt. Dabei benutzt die NSA die Section-702-Befugnis, um an einem Internet-Knoten oder ähnlichen Netzwerkverbindungspunkten direkten Zugang zu den Netzwerken von Telekommunikationsunternehmen

[11] Siehe beispielsweise die detaillierten Minimierungsanforderungen für das Telefonmetadatenprogramm, die in der folgenden, aus der Geheimhaltung herausgenommenen FISC-Entscheidung beschrieben sind: http://www.dni.gov/files/documents/PrimaryOrder Collection 215.pdf

[12] Public Law 95-511, “Foreign Intelligence Surveillance Act of 1978”, http://www.gpo.gov/fdsvs/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf

[13] U.S. Foreign Intelligence Surveillance Court, “Minimization Procedures used by NSA in Connection with FISA Section 702”, 31. Oktober 2011, https://www.aclu.org/sites/default/files/field document/minimization procedures used by nsa in connec tion with fisa sect 702.pdf

[14] Privacy and Civil Liberties Oversight Board, “Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act”, 2. Juli 2014, https://www.pclob.gov/library/702- Report.pdf

zu erhalten. Der gesamte Datenstrom wird mit Selektoren durchsucht und analysiert, und relevante Kommunikationen (einschließlich Telefongesprächen) werden dann in umfangreichen Datenbanken zur anschließenden Verarbeitung gespeichert.

Executive Order 12333 (1981)[15]: Diese Durchführungsverordnung enthält die Vorschriften, denen die Sammlung auslandsnachrichtendienstlicher Informationen durch alle Behörden unterliegt. Sie ersetzt nicht die Bestimmungen des FISA, deckt aber alle Aktivitäten ab, die im FISA nicht behandelt werden.[16] Mit EO 12333 (im Laufe der Jahre dreimal geändert, einschließlich im Jahr 2008) werden die Erfassung auslandsnachrichtendienstlicher Informationen außerhalb der USA genehmigt und Grundsätze und Prioritäten festgelegt. Die Minimierungsverfahren zur Beschränkung der gezielten Überwachung von US-Personen sind weiterhin geheim. Die Aufsicht führen die betreffenden Behörden, das National Security Council und der DNI.

Die weit überwiegende Mehrheit der Auslandsüberwachungsprogramme der NSA[17] wird im Rahmen der Genehmigung durch EO 12333 durchgeführt. In einem offiziellen Überwachungshandbuch aus dem Jahr 2007 heißt es, EO 12333 „ist die Hauptquelle der Befugnisse der NSA zur Sammlung auslandsnachrichtendienstlicher Erkenntnisse."[18] Da die Exekutive die Verordnung erlässt und umsetzt, ist die Beaufsichtigung durch den Kongress oder Gerichte sehr gering. Ein Programm, von dem bekannt ist, dass es mit EO 12333 genehmigt wurde, ist MUSCULAR – ein gemeinsames Projekt von GCHQ und NSA. Es hat das Ziel, in die weltweiten Glasfasernetze einzudringen, die die Datenzentralen von Google, Yahoo und anderen verbinden.[19]

Der gesetzliche Rahmen für die Sammlung auslandsnachrichtendienstlicher Erkenntnisse ist sehr weiträumig und komplex. Die Geheimhaltung hinsichtlich der Interpretation der gesetzlichen Befugnisse durch die NSA und andere Geheimdienststellen, die Geheimhaltung von FISC-Entscheidungen und der Mangel an öffentlichen Informationen über Executive Order 12333 machen eine sorgfältige Bewertung sehr schwierig. Zweifellos basiert jedoch das Rahmenwerk für die Überwachung von Ausländern auf viel schwächeren Normen für die Genehmigung, die Praxis der Durchführung und die Beaufsichtigung als das Rahmenwerk für die Überwachung von US-Personen. Diese Unterteilung ist bei allen Gesetzen vorhanden, die die Zielpersonen von *auslands*nachrichtendienstlicher Aufklärung betreffen, spiegelt aber auch die nur den Bürgern gewährten Grundrechte wider und die separaten rechtlichen Verfahren, wobei für Ermittlungen bei US-Personen wesentlich höhere Schutznormen für die Privatsphäre und die bürgerlichen Freiheiten vorgeschrieben sind.

Teil 2: US-Debatte und Reformanstrengungen

---

[15] Executive Order 12333 - United States Intelligence Activities, http://www.dni.gov/index.php/about/organization/ic-legal-reference-book-2012/ref-book-eo-12333; Scott F. Mann, "Fact Sheet: Executive Order 12333", *Center for Strategic & International Studies*, 24. Februar 2014, http://csis.org/publication/fact-sheet-executive-order-12333-0

[16] *McClatchyDC*, "Most of NSA's data collection authorized by order Ronald Reagan issued", 21. November 2013, http://www.mcclatchydc.com/news/nation-world/national/national- security/article24759289.html

[17] ProPublica, "The NSA Revelations all in one chart", https://projects.propublica.org/nsa-grid/

[18] DOCID 4145825, Overview of Signals Intelligence Authorities, https://www.aclu.org/files/assets/eo12333/NSA/Overview%20of%20Signals%20Intelligence%20Authorities.pdf

[19] Kim Zetter, "Report: NSA Is Intercepting Traffic From Yahoo, Google Data Centers", 30. Oktober 2013, http://www.wired.com/2013/10/nsa-hacked-yahoo-google-cables/

Die Debatte zur Überwachungspolitik war nach den Snowden-Offenlegungen in den USA weit verbreitet und stark beachtet. Rufe nach einer Reform kamen aus dem gesamten politischen Spektrum – von linksorientierten Demokraten ebenso wie von den Republikanern, die den PATRIOT Act verfasst hatten. Zuerst reagierten Dutzende von Unternehmen aus dem Silicon Valley und für bürgerliche Freiheiten eintretende NRO im Juli 2013 mit einem Brief an die Regierungsspitze, in dem sie mehr Transparenz in den Überwachungsprogrammen forderten.[20] Im Dezember 2013 bildete eine aus den führenden amerikanischen Technologieunternehmen bestehende Gruppe eine neue Unternehmenskoalition – die Reform Government Surveillance – und schlug ein Ende der Massenüberwachung sowie eine Reformierung der Aufsichts-, Transparenz- und Durchführungspraxis vor.[21] Im Januar 2013 kamen Briefe von einer Gruppe prominenter Kryptographen und von einer sehr viel größeren Gruppe von Wissenschaftlern hinzu, in denen ein Ende der Massenüberwachung gefordert wurde.[22] Eine Koalition aus zivilgesellschaftlichen Organisationen – ausgerichtet auf bürgerliche Freiheiten, Menschenrechte und Internet-Freiheit –, die Dutzende von Gruppen mit Millionen von Menschen repräsentiert, bildete sich, um auf einen Wandel zu drängen.

Mit der Basiskampagne wurde der Kongress aufgefordert, zwecks Einschränkung der Überwachung das Gesetz zu ändern. An einem einzigen Tag, dem 11. Februar 2014, erreichte die Kampagne 37 Millionen Menschen und erzeugte über eine halbe Million Mitteilungen an den Kongress, Zehntausende Telefonanrufe bei gewählten Amtsträgern und Hunderttausende Unterschriften auf Petitionen.[23] Diese Gruppen sind weiterhin gut organisiert und fordern konsequent einen Wandel in der Gesetzgebung, lassen anspruchsvolle juristische Analysen vornehmen und versuchen, den Kongress zu beeinflussen.[24] Die unternehmerischen und zivilgesellschaftlichen Koalitionen haben sich zusammengeschlossen, um die Verabschiedung des USA Freedom Act voranzutreiben und leisten weiterhin breite parteiübergreifende Unterstützung für ihr Anliegen.

Seit Juni 2013 wurden mehr als 25 Klagen gegen Überwachungsprogramme der US-Regierung eingereicht.[25] NRO wie die American Civil Liberties Union oder die Electronic Frontier Foundation stellen die Legalität verschiedener Programme und die Interpretation zentraler gesetzlicher Rahmenwerke wie des PATRIOT Act oder des Foreign Intelligence Surveillance Act durch die US-Regierung in Frage. Zusätzlich erwirkten Unternehmen wie Google und Yahoo vor Gericht das Recht, in ihren Transparenzberichten mehr Informationen über Datenanforderungen zu veröffentlichen.[26]

Zwar geht es bei einem der bekanntesten Prozesse – ACLU v. Clapper [27] – nur um das inländische Programm zur Erfassung von Telefongesprächen, aber es gibt andere Prozesse, die Auswirkungen auf

---

[20] The New York Times, “Silicon Valley Letter Calling for Surveillance Disclosure”, http://www.nytimes.com/interactive/2013/07/18/us/18nsa-letter.html? r=0

[21] Bei der Abfassung dieses Textes besteht die Gruppe aus AOL, Apple, Dropbox, Evernote, Google, Microsoft und Yahoo: https://www.reformgovernmentsurveillance.com/

[22] April Glaser, “Academics and Researchers Against Mass Surveillance”, *Electronic Frontier Foundation*, 12. Februar 2014, https://www.eff.org/deeplinks/2014/02/academics-and-researchers-against-mass- surveillance

[23] The Day We Fought Back, https://thedaywefightback.org/the-results/

[24] NSA coalition letter, https://www.eff.org/files/2015/03/24/nsa coalition letter 032515.pdf

[25] ProPublica, “NSA Surveillance Lawsuit Tracker”, https://proiects.propublica.org/graphics/surveillance- suits

[26] Center for Democracy and Technology, “Yahoo vs. US PRISM Documents”, https://cdt.org/insight/yahoo-v-u-s-prism-documents/

[27] American Civil LIberties Union, “ACLU v. Clapper - Challenge to NSA Mass Call-Tracking Program”, 3. September 2014, https://www.aclu.org/cases/aclu-v-clapper-challenge-nsa-mass-call-tracking-program

die Persönlichkeitsrechte von Ausländern haben. Beispielsweise focht die Wikimedia Foundation die Legalität des UPSTREAM-Programms der NSA an, das mit Section 702 des Foreign Intelligence Surveillance Act genehmigt wurde.[28] Es gibt eine beeindruckende Zahl von Rechtsfällen, aber die meisten wurden noch nicht angehört oder befinden sich noch in den Vorinstanzen. Auf dem Weg dieser Fälle durch das Rechtssystem könnten die Gerichte eine wichtige Rolle dabei übernehmen, die US-Regierung zur Verabschiedung weiterer Reformen zu drängen. Es ist jedoch unwahrscheinlich, dass US-Gerichte das Diskriminierungsproblem direkt in Angriff nehmen, da sie sich tendenziell auf den Geltungsbereich der gesetzlichen Befugnisse und den Schutz der Grundrechte der US-Bürger konzentrieren.

Die Intensität organisierter Aufforderungen zur Reformierung der Überwachungspolitik in den USA ist in jedem Fall beeindruckend. Ein Großteil dieser Energie war jedoch auf die Begrenzung des (direkten oder indirekten) Abfangens und Sammelns der Daten von Amerikanern gerichtet. Und auch wenn viele Protagonisten in den Reformkoalitionen bereit wären, ihre Unterstützung auf die Persönlichkeitsrechte ausländischer Bürger auszudehnen, sind in der amerikanischen Politikdebatte doch die amerikanischen Persönlichkeitsrechte die wichtigsten Themen. Eine bedeutende Ausnahme von dieser Konzentration auf das Inland sind die Ansichten der amerikanischen Technologie- und Telekommunikationsunternehmen, die in ausländischen Märkten tätig sind. Der nach US-Recht bestehende Zwang, Daten ausländischer Kunden zu übergeben, stellt sie vor ein schwieriges Dilemma. Zur Einhaltung des US-Rechts müssen sie ausländische Gesetze und das Vertrauen ausländischer Kunden verletzen. Aus diesem Grund spielt die wirtschaftliche Dimension der Überwachungsdebatte eine wichtige Rolle in der Entstehung einer international ausgerichteten Reformagenda.

Die Regierung Obama reagierte vielseitig und für politische Änderungen in den USA ungewöhnlich schnell auf diesen öffentlichen Reformdruck. Natürlich stellen die Änderungen in Politik und Praxis kein „Ende der Massenüberwachung“ dar, und sie lösen auch das Diskriminierungsproblem nicht so, dass die Bedenken von Ausländern zerstreut würden. Aber das Gesamtergebnis der Reformen (insbesondere auf dem Gebiet der Transparenz) ist die bedeutendste Änderung in der modernen Informationsgewinnung der USA seit Jahrzehnten.[29] Das politische Pendel, das sich nach dem 11. September in Richtung Maximierung der Sicherheit bewegte, fängt an, in Richtung bürgerliche Freiheiten zurückzuschwingen. Dabei geht es nicht nur um Gesetzesänderungen – obwohl die Gerichte die Rechtswidrigkeit bedeutender Überwachungsprogramme festgestellt haben. Die meisten Änderungen waren nicht notwendig für die Legalität, sondern wurden vorgenommen, um die Legitimität zu stärken und zu fördern.

Aus Gründen der Übersichtlichkeit sind die von der Regierung Obama verabschiedeten Reformen in drei Kategorien unterteilt: 1) Analyse, Überprüfung und Untersuchung von Signalaufklärungsprogrammen durch unabhängige Expertengremien; 2) Änderungen in der Beaufsichtigung, der Transparenz und der Einhaltung von Vorschriften; und 3) breitere Änderungen in Recht und Politik.

---

[28] Michelle Paulson and Geoff Brigham, “Wikimedia v. NSA: Wikimedia Foundation files suit against NSA to challenge upstream mass surveillance”, Wikimedia blog, 10. MArch 2015, http://blog.wikimedia.org/2015/03/10/wikimedia-v-nsa/

[29] Timothy H. Edgar, “The Good News about Spying”, *Foreign Affairs*, 13. April 2015, https://www.foreignaffairs.com/articles/united-states/2015-04-13/good-news-about-spying ; Peter Swire, “The USA FREEDOM Act, the President’s Review Group and the Biggest Intelligence Reform in 40 Years”, *The International Association of Privacy Professionals*, 8. Juni 2015, https://privacyassociation.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest- intelligence-reform-in-40-years

Überprüfung und Untersuchung

Die Snowden-Offenlegungen und die nachfolgende politische Debatte führten zur Bildung und Ermächtigung einer Reihe spezieller Prüfgruppen, Aufsichtsuntersuchungen und wissenschaftlicher Analysen der US-Aufklärungspraxis. Viele wurden von der Bundesregierung in Auftrag gegeben und zahlreiche andere von Privatunternehmen, akademischen Einrichtungen und NRO finanziert. Eine vollständige Übersicht dieser Analysen sprengt den Rahmen dieses Papiers. Ich werde aber drei der wichtigsten von der Regierung finanzierten Bemühungen bezüglich der Beaufsichtigung vorstellen. Sie ergaben jeweils ausführliche Berichte, aus denen die bestehenden Probleme mit Politik und Praxis der Aufklärung ersichtlich wurden. Und es wurden jeweils klare Reformvorschläge gemacht. Viele der Kernempfehlungen sind von direkter Bedeutung für das Thema Privatsphäre und Sicherheitsrechte von Nicht-US-Personen.

President's Review Group on Intelligence and Communications Technologies[30]: Nach den ersten Snowden-Enthüllungen von Juni 2013 richtete das Weiße Haus Mitte August eine spezielle Prüfgruppe ein mit der Aufgabe, die Praxis der Informationserfassung mithilfe von Kommunikationstechnologien zu bewerten, mit Schwerpunkt auf der Bewertung der besten Methoden zum Schutz sowohl der Privatsphäre als auch der Sicherheitsinteressen.[31] Unter den von der Prüfgruppe analysierten Kernfragen waren einige, die für die Persönlichkeitsrechte von Nicht-US-Personen von Bedeutung sind – einschließlich der Verfahren zur Einschränkung der Erfassung, Verarbeitung und Weitergabe von auslandsnachrichtendienstlichen Daten und der Behandlung sicherer Verschlüsselungsstandards im internationalen Markt.

Die fünf Mitglieder der Prüfgruppe waren allesamt ehemalige hochrangige Regierungsbeamte oder Akademiker mit großer Fachkenntnis, Erfahrung und Glaubwürdigkeit bei diesen Themen. Die Arbeit der Prüfgruppe erfolgte sehr zügig (der Abschlussbericht wurde im Dezember 2013 veröffentlicht) und war sehr breit angelegt. Kritiker brachten vor, dass diese Gruppe (zu der ein ehemaliger stellvertretender Direktor der CIA und ein ehemaliger Berater des Weißen Hauses für Terrorismusbekämpfung gehörten) eine „Insider"-Sicht der Sicherheitspolitik repräsentierten, was unweigerlich dazu führe, dass ihre Sichtweisen die Geheimdienststellen begünstigen. Der Abschlussbericht jedoch enthielt 46 detaillierte Reformempfehlungen, die teilweise recht kritisch waren, und mit denen weitreichende Änderungen in der Praxis der Informationserfassung vorgeschlagen wurden. Die Auswirkungen der Tatsache, dass diese Gruppe derart umfassende Reformen forderte, wurden von den Reformbefürwortern gelobt.[32] Es handelt sich um den umfassendsten Entwurf für eine Modernisierung der Sicherheits- und Datenschutzpolitik, der je von einem Aufsichtsgremium geschrieben wurde.

---

[30] Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World", 12. Dezember 2013, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12 rg final report.pdf

[31] Office of the Director of National Intelligence, "The Review Group", http://www.dni.gov/index.php/intelligence-community/review-group

[32] Ellen Nakashima and Ashkan Soltani, "NSA shouldn't keep phone database, review board recommends", *The Washington Post*, 18. Dezember 2013, https://www.washingtonpost.com/world/national-security/nsa-shouldnt-keep-phone-database-review- board-recommends/2013/12/18/f44fe7c0-67fd-11e3-a0b9-249bbb34602c story.html

Die meisten Empfehlungen der Prüfgruppe wurden nicht umgesetzt. Aber diejenigen, die umgesetzt wurden, enthalten ernsthafte Änderungen der Aufklärungspraktiken – beispielsweise ein Ende der Massenerfassung von Telefonmetadaten durch die NSA (siehe unten – USA Freedom Act). Die Empfehlungen zu größerer Transparenz und zur Begrenzung der Massenerfassung (einschließlich ausländischer Quellen) wurden mit der Veröffentlichung von Normen für die Erfassung nachrichtendienstlicher Erkenntnisse, Minimierungspraktiken und Entscheidungen des FISC ebenfalls realisiert (zumindest teilweise).[33] Zu den anderen wichtigen – nicht umgesetzten – Reformvorschlägen des Berichts gehören eine Aufforderung zur Unterstützung starker Verschlüsselung (ohne vorgeschriebene Hintertüren) und eine Empfehlung für verbündete Nationen, Vereinbarungen auszuhandeln, mit denen die Überwachung ausländischer Führungspersönlichkeiten stärker eingeschränkt wird.

Berichte des Privacy and Civil Liberties Oversight Board[34]**.** Der Privacy and Civil Liberties Oversight Board (PCLOB) wurde 2007 mit den Gesetzen zur Umsetzung der Empfehlungen der 9/11-Kommission eingerichtet. Es ist eine unabhängige und parteiübergreifende Einrichtung, deren Aufgabe es ist, die Aktivitäten der US-Regierung in der Terrorismusbekämpfung zu überprüfen, um einen angemessenen Schutz von Privatsphäre und bürgerlichen Freiheiten sicherzustellen. Nach den Snowden-Offenlegungen führte der PCLOB eine Reihe von Expertenanhörungen mit der Teilnahme verschiedener Interessengruppen durch und analysierte die wichtigsten Gesetze, mit denen Signalaufklärung genehmigt wird – einschließlich Section 215 des PATRIOT Act und Section 702 des FISA.[35] Die in zwei größeren Berichten vorgestellten Ergebnisse hatten einen starken Einfluss auf die öffentliche Meinung und die Gestaltung der von den Politikern im Weißen Haus und im Kongress vorgelegten Reformvorschläge. Insbesondere wurde mit dem PCLOB-Bericht über Section 215 ein Ende des Programms empfohlen – ein Vorbote der später mit dem USA Freedom Act verabschiedeten legislativen Lösung. In dem PCLOB-Bericht wurde die juristische Rechtfertigung des Massenerfassungsprogramms kritisiert (was später von einem Bundesgericht anerkannt wurde) und auf die Gefahr hingewiesen, die das Programm für die Persönlichkeitsrechte darstellte, und der Bericht kam zu dem gleichen Schluss wie die White House Review Group, nämlich dass das Programm offenbar von begrenztem Nutzen ist. In der Untersuchung und Analyse der Section-215-Überwachung durch den PCLOB wurde nicht ein einziger Fall identifiziert, in dem das Massenerfassungsprogramm in einer Aktion zur Terrorismusbekämpfung ein wichtiger Faktor gewesen wäre. Die Beachtung der PCLOB-Berichte in den Medien konzentriert sich großenteils auf die Schlussfolgerungen des Board bezüglich der Frage, wie die Persönlichkeitsrechte von US-Personen geschützt werden sollten. Aber die Berichte sind recht wichtig für die umfassendere Frage der Persönlichkeitsrechte auch in der Erfassung auslandsnachrichtendienstlicher Erkenntnisse.

Die PCLOB-Berichte zu Section 215[36] und Section 702[37] wurden im Januar bzw. im Juli 2014 veröffentlicht. Sie enthielten über 20 Reformempfehlungen, die sich an die Exekutive, die Geheimdienststellen, das FISA-Gericht und den US-Kongress richteten. Viele davon sind inzwischen umgesetzt, oder ihre Umsetzung ist im Gange. Im Januar 2015 hat der PCLOB eine Beurteilung der

---

[33] Siehe Fußnote 28
[34] PCLOB, Document Library - Oversight Reports, https://www.pclob.gov/library.html#oversightreports
[35] Zurzeit erfolgt eine Analyse von Executive Order 12333.
[36] PCLOB,"Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court", 23. Januar 2014, https://www.pclob.gov/library/215-Report on the Telephone Records Program.pdf
[37] Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", 2. Juli 2014, https://www.pclob.gov/library/702-Report.pdf

Reaktion der Bundesregierung auf seine Empfehlungen veröffentlicht.[38] Zu den Erfolgen gehören einige Themen, die auch von der Prüfgruppe sowie im USA Freedom Act behandelt werden. Beispielsweise empfahl der PCLOB, dass das FISC unabhängige juristische und technische Experten (einschließlich eines Spezialanwalts für Privatsphäre und bürgerliche Freiheiten) anhören sollte, wenn es Massenerfassungsprogramme überprüft. Der PCLOB empfahl, die Regierung solle FISC-Anordnungen, mit denen neue rechtliche Fragestellungen entschieden werden, veröffentlichen und seine Entscheidungen der Überprüfung durch Berufungsinstanzen unterziehen. Diese Empfehlung schloss sich einer Reihe anderer Empfehlungen zu größerer Transparenz hinsichtlich der Art und Weise, wie durch diese Programme Unternehmen nach aufgezeichneten Daten abgefragt werden, an.

Mit direkterem Bezug zu der Privatsphäre von Nicht-US-Personen empfahl der PCLOB Änderungen in der Art der Beurteilung ausländischer Überwachungsziele im Rahmen von Section 702 durch die NSA. Der PCLOB-Bericht kam zu dem Ergebnis, dass die Zielüberwachungsverfahren bei der Feststellung, ob ein Ziel eine Nicht-US-Person außerhalb der USA ist, sehr genau sind. Aber die Norm für die Beurteilung, ob ein legitimer auslandsnachrichtendienstlicher Zweck vorliegt, war viel geringer. Die Verwaltung stimmte zu, die Norm gemäß der PCLOB-Empfehlung anzuheben. Die Verwaltung akzeptierte auch eine andere PCLOB-Empfehlung, dem FISC zusammen mit dem allgemeinen Antrag auf Zertifizierung breiterer auslandsnachrichtendienstlicher Zwecke auch eine Zufallsauswahl von Beauftragungsbögen mit Informationen zur gezielten Überwachung vorzulegen. Solche Stichproben erlauben eine sorgfältigere Überprüfung der tatsächlichen Praxis und der Selektoren, als wenn die richterliche Prüfung auf höhere Ebenen beschränkt wird. Schließlich erhielt der PCLOB die Zustimmung der Geheimdienste, die Veröffentlichung freigegebener Versionen von Minimierungsverfahren, die von den Behörden benutzt werden, um die Erfassung und Verarbeitung von Kommunikationen unerlaubter Zielpersonen zu vermeiden, vorzubereiten.

Bericht des National Research Council. Unter den Empfehlungen[39] der White House Review Group war ein Vorschlag, eine technische Analyse darüber durchzuführen, wie Software dazu konzipiert werden könnte, die Verwendung von Massenerfassungsmethoden in der Signalaufklärung zugunsten der gezielten Überwachung zu begrenzen. Diese Empfehlung wurde mit der Presidential Policy Directive 28 (Januar 2014) in die Tat umgesetzt. Das Ergebnis war eine vom National Research Council (einem Teil der National Academy of Sciences) im Januar 2015 unter dem Titel *Bulk Collection of Signals Intelligence: Technical Options* veröffentlichte Studie.[40] Der Bericht betrifft die Privatsphäre auslandsnachrichtendienstlicher Zielpersonen, weil er die Notwendigkeit der Massenerfassung (die unbeabsichtigterweise in die Kommunikationen unerlaubter Zielpersonen eindringt) direkt beurteilt und die technischen Optionen zur Begrenzung möglicher Verletzungen der Rechte unerlaubter Zielpersonen untersucht. Der Bericht kommt zu drei Hauptergebnissen.[41] Erstens führt das NRC an, dass Massenerfassung unvermeidlich ist, wenn die Erfassung erfolgt, um einen Datenbestand zu erzeugen, der später ausgewertet werden kann, wenn auslandsnachrichtendienstliche Zielpersonen bekannt werden (z. B. im Rückblick auf erfasste Kommunikationen von Personen, die später als potenzielle Terroristen identifiziert werden). Es wird viel über den Nutzen dieser Theorie der Signalaufklärung als „nachrichtendienstlicher Zeitmaschine“ debattiert, bei der Heuhaufen von Daten gesammelt werden, damit

[38] PCLOB, “Recommendations Assessment Report”, 29. Januar 2015, https://www.pclob.gov/library/Recommendations Assessment-Report.pdf
[39] Siehe op. cit., Fußnote 30 (Seite 33, Empfehlung 20).
[40] National Research Council, “Bulk Collection of Signals Intelligence: Technical Options”, 15. Januar 2015, http://www.nap.edu/openbook.php?record id=19414
[41] Andy Wang, “The NRC's Bulk Collection Report: a High-Level Overview”, *Lawfare*, 20. Januar 2015, http://www.lawfareblog.com/nrcs-bulk-collection-report-high-level-overview

irgendwann in der Zukunft nach Nadeln gesucht werden kann.[42] Aber der NRC-Bericht kommt zu dem Ergebnis, dass es keine technische Alternative gibt. Zweitens wird in dem Bericht angeführt, dass trotz der Erkenntnis, dass Massenerfassung nicht durch Software zu vermeiden ist, die einen gezielteren Ansatz ermöglicht, eine Verbesserung der Einschränkungen der Privatsphäre bei bestimmten Überwachungsaktionen technisch möglich wäre. Beschränkungen von Abfragen, Zugang, Datenkombinationen und Verbreitung können fest in die Software eingebaut werden, damit Verletzungen durch menschliche Fehler oder absichtlichen Missbrauch verhindert werden. Schließlich kommt der Bericht zu dem Ergebnis, dass die weitere Entwicklung von Software die Filtertechnologien, mit denen Daten, die für die Suchbegriffe irrelevant sind, automatisch gelöscht werden, verbessern und somit de facto einen gezielteren Ansatz für die Massenerfassung schaffen könnte.

Beaufsichtigung, Transparenz und Einhaltung von Vorschriften

Teilweise als Reaktion auf die Analyse und die Empfehlungen der Berichte der Prüfgruppe und des PCLOB haben die US-Geheimdienste (Intelligence Community, IC) erstmals einen Prozess in Gang gesetzt, mit dem der Öffentlichkeit mehr Transparenz hinsichtlich ihrer Aktionen geboten wird – auch bei Angelegenheiten, die direkt oder indirekt mit den Persönlichkeitsrechten von Nicht-US-Personen zusammenhängen. Auf einer neuen Internetseite mit der Bezeichnung „IC on the Record“ haben die Behörden eine Vielzahl von Dokumenten und Erklärungen bezüglich gesetzlicher Genehmigung, Praxis der Durchführung, Minimierungsverfahren und Aufsichtsmethoden veröffentlicht. Ein bedeutender Teil des Inhalts geht auf in der Presidential Policy Directive 28 (siehe unten) enthaltene Anordnungen zurück, nach denen die IC Richtlinien und Verfahren so revidieren müssen, dass der Schutz der Privatsphäre verbessert wird und persönliche Informationen geschützt werden. Zusätzlich haben die Geheimdienststellen eine Reihe spezifischer Reformen der Arbeitsabläufe eingeführt, von denen mehrere auch Aufsicht, Schulung und Transparenz betreffen. Schließlich ist auch erwähnenswert, dass das National Institute of Standards and Technology (NIST) – eine Einrichtung des Wirtschaftsministeriums, die sich von Sicherheitsexperten sagen lassen musste, dass sie einen kryptographischen Standard unterstützte, der als von der NSA kompromittiert angesehen wurde[43] – die Zweifel an der Richtigkeit seiner Arbeit durch Änderung seiner Empfehlungen zur Kryptographie beseitigt hat.[44]

IC on the Record[45]: Die von dem Office of the Director of National Intelligence unterhaltene Tumblr-Site wurde auf Anweisung des Präsidenten geschaffen. Sie dient dazu, Sachinformationen über die Tätigkeit der Erfassung auslandsnachrichtendienstlicher Erkenntnisse zu veröffentlichen, um die Transparenz zu erhöhen. Sie enthält freigegebene Dokumente, offizielle Stellungnahmen, Aussagen von Führungspersonen vor dem Kongress, Reden, Informationsblätter und den neuen Jahresbericht, in dem die von den IC zur Reform ihrer Praktiken zwecks besseren Schutzes von Privatsphäre und bürgerlichen Freiheiten unternommenen Schritte dokumentiert sind. Unter dem beachtenswerten Inhalt dieser Site befinden sich einige Texte, die für die Persönlichkeitsrechte von Nicht-US-Personen von Bedeutung sind. Dazu gehören:

[42] Marshall Erwin, “The Intelligence Time Machine”, *JustSecurity*, 30. April 2015, http://iustsecurity.org/22560/intelligence-time-machine/
[43] Michael Mimoso, “In Wake of Latest Crypto Revelations, ‘Everything is Suspect’”, *ThreatPost*, 20. September 2013, https://threatpost.com/in-wake-of-latest-crypto-revelations-everything-is- suspect/102377
[44] Dennis Fisher, “NIST Drops Weak Dual_EC RNG From Official Recommendations”, *ThreatPost*, 26. Juni 2015, https://threatpost.com/nist-drops-weak-dual ec-rng-from-official-recommendations/113493
[45] Office of the Director of National Intelligence - IC on the Record, http://icontherecord.tumblr.com/

- *IC-Transparenzberichte.*[46] Die IC haben mit der Veröffentlichung jährlicher Transparenzberichte begonnen, in denen Daten wie die Anzahl der in einem bestimmten Jahr gewährten FISA-Anordnungen und die Anzahl der betroffenen Zielpersonen angegeben sind. Die reinen Zahlen geben keinen besonderen Einblick, weil aus ihnen nicht die Anzahl der von bestimmten Anordnungen oder Ziellisten betroffenen Nicht-US-Personen ersichtlich ist. Trotzdem handelt es sich um ein vorher bei auslandsnachrichtendienstlichen Aktionen nie dagewesenes Transparenzniveau.

- *Supplemental Privacy Procedures der NSA.*[47] Alle Stellen der IC haben (wie nach PPD 28 vorgeschrieben) neue Leitlinien erstellt, mit denen die Verfahren zum Schutz persönlicher Informationen – einschließlich speziell der persönlichen Informationen von Nicht-US-Personen – aktualisiert und verbessert werden. In diesen zusätzlichen Leitlinien wird angeregt, die Privatsphäre von Nicht-US-Personen, soweit dies „mit der nationalen Sicherheit vereinbar" ist, ähnlich zu behandeln wie diejenige von US-Personen. Diese Verfahren sind offenbar eine direkte Erklärung der Übereinstimmung mit bestehendem Recht. Aber die Veröffentlichung dieser Verfahren stellt einen bemerkenswerten Grad von Transparenz dar. In den umfangreichen Änderungen kommen die Anforderungen der Richtlinie des Präsidenten, einschließlich der Vorschrift, Daten von Nicht-US-Personen nach 5 Jahren zu löschen (es sei denn, sie sind eigens von dem ODNI ausgenommen oder verschlüsselt), zum Ausdruck. Vorher war die Dauer der Datenaufbewahrung bei den verschiedenen IC unterschiedlich – jetzt beträgt sie mit den genannten Ausnahmen einheitlich 5 Jahre. Diese Begrenzung wird von manchen Sicherheitsanalytikern als erhebliche neue Einschränkung angesehen.[48]

- *Freigegebene betriebliche Dokumente.*[49] Die IC haben eine Reihe von Informationsdokumenten über ihre Arbeit aus der Geheimhaltung herausgenommen und veröffentlicht. Dazu gehören – als Beispiele – die Minimierungsverfahren von NSA[50] und CIA[51] für die Löschung, Verarbeitung, Weitergabe und Speicherung von Daten von Ausländern, die im Rahmen von Section 702 des FISA erfasst wurden.

- *Freigegebene FISC-Entscheidungen.* Auf die Empfehlung des PCLOB hin haben die IC begonnen, frühere FISC-Stellungnahmen, die sich mit neuen rechtlichen und technologischen Fragestellungen auseinandersetzen, freizugeben und zu veröffentlichen. Außerdem befinden sie sich angeblich in einem Freigabeprozess für aktuelle Entscheidungen, die sich mit neuen rechtlichen und technologischen Fragestellungen auseinandersetzen.[52]

---

[46] IC on the Record, "Calendar Year 2014 Transparency Report", 22. April 2015, http://icontherecord.tumblr.com/transparency/odni transparencyreport cy2014
[47] National Security Agency, "PPD-28 Section 4 Procedures", 12. Januar 2015, https://www.nsa.gov/public info/ files/nsacss policies/PPD-28.pdf
[48] Carrie Cordero, "First Take on Government's Surveillance Reform Update Report", *Lawfare*, 4. Februar 2015, http://www.lawfareblog.com/first-take-governments-surveillance-reform-update-report
[49] IC on the Record, "Release of Documents Concerning Activities under the Foreign Intelligence Surveillance Act", 3. März 2015, http://icontherecord.tumblr.com/post/112610953998/release-of- documents-concerning-activities-under
[50] Foreign Intelligence Surveillance Court, "Standard Minimization Procedures for Electronic Surveillance Conducted by the National Security Agency (NSA)", 13. Dezember 2006, http://www.dni.gov/files/documents/0315/NSA%20Minimization%20Procedures.pdf
[51] Foreign Intelligence Surveillance Court, "CIA Minimization Procedures for Information from FISA Electronic Surveillance conducted by NSA", 13. Dezember 2006, http://www.dni.gov/files/documents/0315/CIA%20Minimization%20Procedures.pdf
[52] Siehe Fußnote 39 (Seite 9-10).

Verfahrens- und Betriebsänderungen. Neben der Erhöhung der Transparenz haben die IC eine Reihe von Änderungen an ihrer Arbeitsweise vorgenommen, die erwähnenswert sind, weil sie zum Teil direkt den Schutz persönlicher Informationen von Nicht-US-Personen betreffen.[53]

- *Begrenzung der Erfassung im Rahmen von Section 702.* Als Reaktion auf den PCLOB-Bericht zu Section 702 hat das ODNI Verfahrensänderungen angeordnet. Dazu gehört eine Änderung des Arbeitsablaufs, nach der der Analytiker zusätzlich dokumentieren muss, dass die Zielperson nicht nur eine US-Person außerhalb der USA ist, sondern auch, dass die Kommunikationen der Zielperson von auslandsnachrichtendienstlichem Wert sind (vorher war die letztgenannte Dokumentation nicht erforderlich). Eine weitere Änderung ist die Beschränkung für eine länger als 5 Jahre andauernde Speicherung der Daten ohne spezifische Genehmigung des ODNI.[54]

- *Stärkere Beaufsichtigung problematischer Erfassungstätigkeiten durch das Weiße Haus.* Das Weiße Haus hat in der PPD 28 angekündigt, dass es aktiv eingreifen wird, um einseitige Entscheidungen der IC über eine gezielte Überwachung bei problematischen Erfassungstätigkeiten zu vermeiden. Insbesondere werden bei solchen Entscheidungen wirtschaftliche und diplomatische Entscheidungsträger innerhalb der Regierung zu Rate gezogen. Zu den problematischen Themen gehört die Überwachung ausländischer Führungspersönlichkeiten.

- *Erhöhung der Finanzierung für den PCLOB und MLAT-Bearbeitung.* Budgetanträge von der Verwaltung und Ausgabengesetzentwürfe im Kongress würden die Mittel für die Tätigkeit des PCLOB[55] wie auch für die Bearbeitung von Anträgen im Rahmen von Rechtshilfeabkommen (Mutual Legal Assistance Treaty, MLAT) durch das Justizministerium beträchtlich erhöhen.[56] (MLAT sind Abkommen, die grenzüberschreitende strafrechtliche Ermittlungen einschließlich Datenanforderungen ermöglichen.) Es handelt sich um wichtige institutionelle Reformen mit dem Zweck, sicherzustellen, dass Aufsicht und Aufmerksamkeit bezüglich der Sicherung der Privatsphäre von Nicht-US-Personen angemessen bleiben und nicht nachlassen.

NIST-Standards für Kryptographie. Außer den Änderungen bei den IC gibt es damit verbundene institutionelle Reformen. Das National Institute for Standards and Technology hat beispielsweise einen Standard für die Erzeugung von Zufallszahlen aus seinen offiziellen Empfehlungen entfernt.[57] Dieser Standard war vorher von Kryptographie-Experten scharf kritisiert worden, die ihn als zu schwach zur

---

[53] Peter Swire, "Preparing to Debate NSA Surveillance and Online Commercial Tracking", *The International Association of Privacy Professionals*, 18. Februar 2015, https://privacyassociation.org/news/a/preparing-to-debate-on-nsa-surveillance-and-online-commercial-tracking/

[54] Alex Ely, "DNI Report on Implementation of Signals Intelligence Reforms: Some Highlights", *Lawfare*, 8. Februar 2015, http://www.lawfareblog.com/dni-report-implementation-signals-intelligence-reforms-some- highlights

[55] Julian Hatten, "Spending bill more than doubles money for privacy watchdog", *The Hill*, 9. Dezember 2014, http://thehill.com/policy/technology/226574-spending-bill-more-than-doubles-money-for-privacy- watchdog

[56] US Department of Justice, "Mutual Legal Assistance Treaty Process Reform", *FY 2015 Budget Request*, http://www.justice.gov/sites/default/files/imd/legacy/2014/07/13/mut-legal-assist.pdf

[57] The National Institute of Standards and Technology (NIST), "NIST Revises Key Computer Security Publication on Random Number Generation", 25. Juni 2015, http://www.nist.gov/itl/csd/random- number-generation.cfm

Gewährleistung der Sicherheit und möglicherweise durch Teilnahme der NSA in den mit der Standardsetzung befassten Arbeitsgruppen absichtlich kompromittiert bezeichneten.[58] Eine kürzlich vorgenommene Änderung an einem Ausgabengesetzentwurf des Repräsentantenhauses würde es dem NIST ausdrücklich verbieten, sich mit NSA oder CIA hinsichtlich seiner Arbeit mit kryptographischen Standards zu beraten.[59]

Neue Politik

Presidential Policy Directive 28[60]. Die bedeutendste Änderung in der Politik der Bundesregierung bezüglich der Erfassung auslandsnachrichtendienstlicher Erkenntnisse und der bei Nicht-US-Personen angewandten Datenschutzstandards wurde mit PPD 28 in Kraft gesetzt. Die PPD 28, die von Präsident Obama in einer größeren Rede[61] über die NSA, die Privatsphäre und die Sicherheitspolitik angekündigt wurde, enthält reformierte Leitlinien und Anforderungen für die von US-Behörden betriebene Signalaufklärung.[62] Sie ist das einzige Dokument seiner Art weltweit, das öffentlich ist.[63] Die Rede ist in erster Linie eine Verteidigung der Praktiken der IC und steht im Einklang mit den amerikanischen Werten. Aber sie erkennt an, dass eine Modernisierung und eine Justierung der Praktiken und Vorgehensweisen notwendig sind, um das Vertrauen in die Glaubwürdigkeit der Schutzbestimmungen für die Privatsphäre wiederherzustellen – nicht nur für Amerikaner, sondern für alle Völker weltweit. Die PPD 28 ist keine politische Änderung, mit der größere gesetzliche Änderungen an als gesetzwidrig geltenden Programmen vorgenommen werden sollen, sondern vielmehr eine Richtlinie, mit der die Legitimität durch Transparenz, Aufsicht und höhere Normen wiederhergestellt werden soll, damit persönliche Informationen geschützt und die Nutzung der mächtigen Instrumente der Signalaufklärung auf sehr spezifische Zwecke beschränkt wird.

Die wichtigsten Bestimmungen der PPD 28 mit Bezug zu Schutzmaßnahmen für die Privatsphäre von Ausländern sind die folgenden, von denen viele schon Gesetz waren, die aber jetzt klar in einem einzigen Dokument niedergelegt sind:

Begrenzung auf bestimmte Zwecke. In der PPD 28 sind ausschließliche Zwecke festgelegt, für die eine Massenerfassung von Nachrichtensignalen erlaubt werden kann.

---

[58] Mike Masnick, “NSA & GCHQ Covertly Took Over Security Standards, Recruited Telco Employees To Insert Backdoors”, *techdirt*, 5. September 2013, https://www.techdirt.com/articles/20130905/12295324417/nsa-gchq-covertlv-took-over-securitv- standards-recruited-telco-employees-to-insert-backdoors.shtml

[59] Amendment to H.R. 2578, offered by Mr. Massie of Kentucky, 3. Juni 2015, http://repcloakroom.house.gov/uploadedfiles/cis16massie4.pdf

[60] The White House - Office of the Press Secretary, “Presidential Policy Directive -- Signals Intelligence Activities”, 17. Januar 2014, https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy- directive-signals-intelligence-activities

[61] The White House - Office of the Press Secretary, “Remarks by the President on Review of Signals Intelligence”, 17. Januar 2014, https://www.whitehouse.gov/the-press-office/2014/01/17/remarks- president-review-signals-intelligence

[62] Mark Landler and Charlie Savage, “Obama Outlines Calibrated Curbs on Phone Spying”, *The New York Times*, 17. Januar 2014, http://www.nytimes.com/2014/01/18/us/politics/obama-nsa.html? r=1

[63] Benjamin Wittes, “The President's Speech and PPD-28: A Guide for the Perplexed”, *Lawfare*, 20. Januar 2014, http://www.lawfareblog.com/presidents-speech-and-ppd-28-guide-perplexed

> *(1) gegen die USA und ihre Interessen gerichtete Spionage und andere Bedrohungen und Aktivitäten fremder Mächte oder ihrer Geheimdienste; (2) Bedrohungen der USA und ihrer Interessen durch Terrorismus; (3) Bedrohungen der USA und ihrer Interessen durch Entwicklung, Besitz, Verbreitung oder Einsatz von Massenvernichtungswaffen; (4) Bedrohungen der Cyber-Sicherheit; (5) Bedrohungen der US-Streitkräfte oder alliierter Streitkräfte oder anderen US-Personals oder alliierten Personals; und (6) transnationale kriminelle Bedrohungen, einschließlich der unerlaubten Finanzierung und der Umgehung von Sanktionen im Zusammenhang mit den anderen in diesem Abschnitt genannten Zwecken.*

Grundsätze des Datenschutzes und der bürgerlichen Freiheiten. Die PPD 28 verbietet die Erfassung auslandsnachrichtendienstlicher Informationen zum Zweck der Unterdrückung politischen Widerspruchs oder „zur Benachteiligung von Personen aufgrund ihrer Volkszugehörigkeit, ihrer Rasse, ihres Geschlechts, ihrer sexuellen Orientierung oder Religion“. Diese Grundsätze werden allgemein angewandt.*Alle Personen sind mit Würde und Respekt zu behandeln, unabhängig von ihrer Nationalität oder ihrem Wohnsitz, und alle Personen haben beim Umgang mit ihren persönlichen Informationen ein berechtigtes Interesse hinsichtlich ihrer Privatsphäre. US-Signalaufklärungsaktivitäten müssen daher angemessene Schutzvorkehrungen für die persönlichen Informationen aller natürlichen Personen umfassen, unabhängig von der Nationalität des Einzelnen, auf den sich die Information bezieht, oder seinem Wohnort.*

Verbot der Industriespionage. Mit PPD 28 wird ausdrücklich die Erfassung und Verbreitung von nachrichtendienstlichen Informationen zum Zwecke der kommerziellen Begünstigung geschäftlicher Interessen der USA verboten.

Absicherungen und Verfahren zum Schutz der Privatsphäre. Mit Section 4 der PPD 28 werden die IC angewiesen, ihre Datenschutzstandards und Absicherungen „im größtmöglichen Umfang, der mit der nationalen Sicherheit vereinbar ist“ auf alle Personen anzuwenden, unabhängig von ihrer Nationalität. Dazu gehört ein Minimierungsverfahren, mit dem die Aufbewahrung persönlicher Daten auf 5 Jahre begrenzt und die Verbreitung persönlicher Daten auf den Standard beschränkt wird, der auch für vergleichbare Informationen von US-Personen gilt (wobei es sich allerdings nicht um einen besonders strengen Standard handelt)[64]. Persönliche Daten müssen unter sicheren Bedingungen aufbewahrt werden, um unberechtigten Zugriff zu verhindern, und persönliche Daten werden nur dann in den nachrichtendienstlichen Berichten verwendet, wenn diese Daten einen konkreten auslandsnachrichtendienstlichen Wert besitzen. Und schließlich werden mit dieser Section eine neuerliche Betonung auf die Beaufsichtigung vorgeschrieben und eine Reihe von Berichten über die Umsetzung dieser Richtlinien durch die IC in den nachfolgenden Monaten angeordnet.

Koordinator für Internationale Diplomatie. Mit PPD 28 wird außerdem der Außenminister angewiesen, einen hochrangigen Beamten zu benennen, der als Schnittstelle zu allen fremden Regierungen dient, die Bedenken bezüglich der US-Signalaufklärungspolitik anmelden wollen.[65]

Die PPD 28 ist ein außerordentliches Dokument, obwohl es nur relativ wenige bedeutende Änderungen an Politik und Praxis enthält. Nach ihm gelten allgemeine Grundsätze des Datenschutzes und der bürgerlichen Freiheiten für die Erfassung nachrichtendienstlicher Informationen, unabhängig von der Nationalität. Es begrenzt die Massenerfassung in der Signalaufklärung auf spezifische Zwecke. Und es

---

[64] Executive Order 12333 - United States intelligence activities, 2.3 Collection of Information, http://www.archives.gov/federal-register/codification/executive-order/12333.html#2.3

[65] Diese Aufgabe wurde dem Undersecretary for Economic Growth, Energy and the Environment übertragen.

schreibt – vorbehaltlich nationaler Sicherheitsinteressen – Verfahren und Normen vor, nach denen für die Absicherung der Privatsphäre von Nicht-US-Personen das gleiche Niveau gilt wie bei US-Personen. Es ist ein Basisdokument, mit dem Normen für die gesetzliche Legitimität festgelegt werden sollen. Alle künftigen Reformen werden daran gemessen werden; sie werden nach ihm beurteilt, und sie werden darauf aufbauen.

USA Freedom Act (2015)[66]. Eine der ersten Problembehandlungen nach der Offenlegung geheimer Dokumente durch Edward Snowden konzentrierte sich auf das Massenerfassungsprogramm, das es der NSA erlaubte, ALLE Metadaten aller Telefongespräche in den USA zu erfassen, zu speichern und abzufragen. Angeblicher Zweck war es, das Abfangen von Anrufen mit auslandsnachrichtendienstlichem Wert bei oder von Nicht-US-Personen außerhalb der USA sicherzustellen. Die Ermächtigung zu diesem Massenerfassungsprogramm kam von Section 215 des PATRIOT Act – einer gesetzlichen Bestimmung, die benutzt werden kann, um private Unternehmen dazu zu zwingen, Geschäftsunterlagen oder „greifbare Dinge" zu übergeben. Der Anwendungsumfang des Gesetzes nach Auslegung der NSA wurde mit einer umstrittenen FISC-Entscheidung genehmigt.

Die Legalität des Programms wurde (sowohl auf gesetzlicher als auch auf verfassungsrechtlicher Basis) bald vor Gericht angefochten. Und letztlich – fast zwei Jahre später – entschied ein Bundesberufungsgericht, dass das Programm in der vom FISC genehmigten Form keine dem Gesetz entsprechende Auslegung von Section 215 ist.[67] (Dieses Gericht eröffnete auch die neue Möglichkeit, dass vorher geheime FISC-Entscheidungen im normalen Verlauf von Berufungsverfahren revidiert werden können.) Vor den Gerichtsentscheidungen überprüften sowohl die White House Review Group als auch der PCLOB das Section-215-Programm und empfahlen seine Beendigung oder zumindest größere Änderungen seines Betriebs, nach denen keine weitere Erfassung und Speicherung von Massenaufzeichnungen von Metadaten mehr erlaubt würde. In der politischen Debatte konzentrierten sich die Einwendungen gegen das Programm weitgehend auf die breite Erfassung von Metadatensätzen von US-Personen (in der Verfolgung von Kommunikationen von Nicht-US-Personen). Eine größere Reform des Metadatenprogramms nach Section 215 würde sich aber auch günstig auf die Persönlichkeitsrechte von Nicht-US-Personen auswirken, deren Datensätze auch bei Fehlen eines auslandsnachrichtendienstlichen Zwecks bei der Massenerfassung miterfasst wurden.

Im Frühjahr 2015 beendete der Kongress diese Debatte nach mehreren Fehlstarts mit der Verabschiedung des USA Freedom Act, eines parteiübergreifenden Gesetzentwurfs, der vom Weißen Haus, von der Technologiebranche und von vielen Bürgerrechtsorganisationen unterstützt wurde. Dies ist die erste vom Kongress verabschiedete bedeutende Einschränkung der nachrichtendienstlichen Erfassungspraktiken seit mehr als 30 Jahren. Die Gesetzgebung änderte nicht nur grundlegend das Metadatenerfassungsprogramm, sondern sie leitete auch eine Reihe weiterer wichtiger Reformen der nachrichtendienstlichen Praxis ein. Nachstehende Bestimmungen des USA Freedom Act sind direkt oder indirekt von Bedeutung für die Privatsphäre und die bürgerlichen Freiheiten von Nicht-US-Personen[68]:

---

[66] H.R. 2048 - USA FREEDOM Act of 2015, 2. June 2015, https://www.congress.gov/bill/114th- congress/house-bill/2048/text

[67] Charlie Savage and Jonathan Weisman, "N.S.A. Collection of Bulk Call Data Is Ruled Illegal", *The New York Times*, 7. Mai 2015, http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled- illegal-by-appeals-court.html; US Court of Appeals for the Second Circuit, "ACLU v. Clapper", 7. Mai 2015, http://www.ca2.uscourts.gov/decisions/isvsquerv/5b758b27-c77d-44a2-b6e5-dbf456f5c142/1/doc/14- 42 complete opn.pdf

[68] US House of Representatives - Judiciary Committee, "USA Freedom Act", 3. Juni 2015, http://iudiciary.house.gov/index.cfm/usa-freedom-act

- Verbot der Erfassung *aller* Metadatensätze sowie die Beschränkung, dass Suchbegriffe für eine Massenerfassung, die zur Genehmigung eingereicht werden, nicht ohne Unterscheidung sein dürfen (wie z. B. alle Datensätze einer bestimmten Stadt). Die Metadatensätze werden von den Telekommunikationsunternehmen gespeichert (nicht von der Behörde) und dürfen erst nach einer juristischen Einzelfallprüfung von den Sicherheitsbehörden abgefragt werden.[69]
- Erlaubnis für Unternehmen, „Maulkorbanordnungen" anzufechten, die es ihnen verbieten, Nichtoffenlegungsanforderungen zu verletzen, die in zur Erzwingung von Kommunikationsdaten ausgestellten National Security Letters enthalten sind. Für Technologieunternehmen ist auch mehr Transparenz bezüglich der Veröffentlichung von Anzahl und Art der Datenanforderungen erlaubt.
- Schaffung eines Gremiums aus Experten für Privatsphäre, bürgerliche Freiheiten und Technologie, das dem FISA-Gericht Beratung und Orientierung bieten soll.
- Vorschrift der Freigabe von Gutachten des FISA-Gerichts, die neue Gesetzesauslegungen, einschließlich des festgelegten Anwendungsbereichs von Suchbegriffen, enthalten.

Mit dem USA Freedom Act werden viele der anfänglich in dem Bericht der White House Review Group und in der Überprüfung des Section-215-Programms durch den PCLOB gegebenen Empfehlungen gesetzlich festgeschrieben. Dazu gehören die Abschaffung der bei der Regierung gespeicherten Massenerfassung von Metadaten, eine höhere Norm der juristischen Überprüfung, Begrenzungen für National Security Letters, mehr Transparenz beim FISC und die Versorgung des Gerichts mit sachverständigen und kontradiktorischen Ansichten von Technologen und Verfechtern bürgerlicher Freiheiten.[70]

Judicial Redress Act (2015).[71] Mitte 2014 kündigte der damalige Justizminister Eric Holder an, die Regierung Obama werde mit dem Kongress zusammenarbeiten, um ein Gesetz zu verabschieden, mit dem EU-Bürgern das Recht gewährt wird, vor US-Gerichten genauso Schadenersatz nach dem Privacy Act von 1974 geltend zu machen wie US-Bürger.[72] Dieses Recht werde für EU-Bürger einen Rechtsbehelf darstellen, wenn persönliche Daten, die von ihren Heimatländern an die US-Regierung weitergegeben wurden, in gesetzwidriger Weise offengelegt wurden.

Danach wurden sowohl ins Repräsentantenhaus als auch in den US-Senat Rechtsvorschriften mit der Bezeichnung Judicial Redress Act of 2015 eingebracht. Dieser Gesetzentwurf würde, falls verabschiedet, den Nutzen des Privacy Act von 1974 auf alle Bürger wichtiger US-Verbündeten ausdehnen, die vor US-

---

[69] The Washington Post, "USA Freedom Act: What's in, what's out", 2. Juni 2015, http://www.washingtonpost.com/graphics/politics/usa-freedom-act/
Bei privaten Fernsprechteilnehmern geht die Befugnis der Massenerfassung über Metadaten hinaus und lässt „zwei Sprünge" bei Kommunikationsaufzeichnungen bezüglich einer Zielperson zu (d.h. alle Nummern, die Kontakt zu der Zielperson haben, und alle Nummern, die Kontakt zu den Nummern haben, die Kontakt zu der Zielperson haben).
[70] Siehe Fußnote 30.
[71] H.R.1428 - Judicial Redress Act of 2015, https://www.congress.gov/bill/114th-congress/house-bill/1428
[72] US Department of Justice, "Attorney General Holder Pledges Support for Legislation to Provide E.U. Citizens with Judicial Redress in Cases of Wrongful Disclosure of Their Personal Data Transferred to the U.S. for Law Enforcement Purposes", 25. Juni 2014, http://www.iustice.gov/opa/pr/attorney-general- holder-pledges-support-legislation-provide-eu-citizens-iudicial-redress

Gerichten Schadenersatz dafür geltend machen, dass ihre Persönlichkeitsrechte von einer Behörde der US-Regierung verletzt werden. Dieses Recht wird umgekehrt in vielen Fällen schon US-Bürgern gewährt, die europäische Gerichte anrufen. Mit dem Gesetz soll allen verbündeten Ländern, die für die Zwecke der gegenseitigen Strafverfolgung Informationen mit der US-Regierung austauschen, Vertrauen und Sicherheit gegeben werden.[73]

Teil 3: Fazit – Eine gemeinsame Suche nach Legitimität

In den USA hat in den letzten zwei Jahren eine eingehende Debatte über die Standards für Privatsphäre und bürgerliche Freiheiten bei der Erfassung nachrichtendienstlicher Informationen stattgefunden. Und während ein großer Teil dieser Debatte sich darauf konzentrierte, wie durch die US-Aufklärung (bei der Verfolgung auslandsnachrichtendienstlicher Zielpersonen) die Persönlichkeitsrechte von US-Personen verletzt werden, wurde auch der Wiederherstellung des Vertrauens in die Legitimität des US-Rechts, dem die Überwachung ausländischer Bürger unterliegt, erhebliche Beachtung zuteil. Die von der Regierung Obama und dem US-Kongress vorgeschlagenen und eingeleiteten Reformen haben den Abstand zwischen den für US-Bürger und Nicht-US-Bürger geltenden Normen verkleinert, aber er ist immer noch groß.

Wenige Europäer würden die Behauptung unterstützen, die politischen Reformen der Praktiken der USA in der Erfassung nachrichtendienstlicher Informationen seien ausreichend, um ihre Bedenken zu zerstreuen; aber es ist nicht zu leugnen, dass Washington zahlreiche Anstrengungen für einen Wandel unternommen hat. Keine dieser Anstrengungen ist einzeln eine entscheidende Änderung des Ansatzes. Das Diskriminierungsproblem, das ich als ein Hauptproblem aus deutscher Sicht bezeichnet habe, bleibt eine große Herausforderung. Aber der kumulative Effekt der Überprüfungen, Untersuchungen, Verfahrensänderungen, verbesserten Standards, Transparenz und öffentlichen Dokumentation von Politik und Praxis der Regierung Obama ergibt insgesamt eine Grundlinie für die globale Datenschutz- und Sicherheitspolitik. Alle künftigen Reformanstrengungen innerhalb und außerhalb der USA werden an dieser Grundlinie gemessen werden.

Kein Land kann glaubwürdig eine Reform oder mehr Legitimität fordern, wenn es nicht die von der Regierung Obama geschaffene Grundlinie erreicht oder übertroffen hat. Auch wenn es eine unbequeme Wahrheit in der europäischen Reaktion auf die Snowden-Offenlegungen ist, so haben doch viele europäische Länder sich bisher gesträubt, ihre eigenen Praktiken kritisch unter die Lupe zu nehmen. Zwar hat jeder, der sich Sorgen um die Privatsphäre macht, gute Gründe, bezüglich der Überwachung durch die NSA beunruhigt zu sein, aber die Zurückhaltung europäischer Länder gegenüber einer intensiven Debatte über ihre eigenen Praktiken und das Versäumnis, höhere Standards für legitime gesetzliche Rahmenwerke zu setzen, bringen europäische Regierungen in eine schwache Position, wenn es um die Anfechtung von US-Praktiken geht.

Dank der Arbeit dieses Ausschusses hat in Deutschland eine intensive Debatte über die gesetzlichen Rahmenwerke für den BND sowie seine betrieblichen Praktiken und seine Beaufsichtigung stattgefunden. Die Faktenermittlungstätigkeit des Ausschusses ähnelt derjenigen, die in die Berichte der White House Review Group und des Privacy and Civil Liberties Oversight Board einfloss. Er hat Experten angehört, Praktiken und gesetzliche Rahmenwerke untersucht und die Transparenz erhöht. Insbesondere hat der Ausschuss – ganz ähnlich wie die Prüfgruppe und der PCLOB – bedeutende gesetzliche Mängel in der

[73] Chris Murphy, “Murphy, Hatch introduce Judicial Redress Act of 2015”, 17. Juni 2015, http://www.murphv.senate.gov/newsroom/press-releases/murphv-hatch-introduce-iudicial-redress-act-of- 2015

Genehmigung der vom BND vorgenommenen Auslandsüberwachung entdeckt.[74] Und der Ausschuss hat eine große Diskrepanz zwischen dem festgestellt, was die Öffentlichkeit und ihre Repräsentanten über Überwachungspraktiken wissen, und dem, was tatsächlich im digitalen Zeitalter mit erweiterten technologischen Fähigkeiten geschieht.

Die Schlüsselfrage ist, ob und wie Deutschland die von diesem Ausschuss entdeckten Probleme behandelt. Sinnvolle Reformen würden Deutschland von anderen europäischen Ländern abheben und in eine Position bringen, in der es auf der Grundlage einer höheren Norm als erstes Land die Überwachungsnormen und -praktiken der USA anfechten könnte. Aus meiner Sicht sollte die Reformagenda die folgenden Punkte enthalten.[75]

- Ausdehnung des G10-Gesetzes und der G10-Genehmigungsverfahren auf alle Überwachungsprogramme;
- Stärkung der Überwachungsfähigkeiten der G10-Kommission, einschließlich der Teilnahme eines Verfechters der bürgerlichen Freiheiten bei der Prüfung von Genehmigungsanträgen und der Unterstützung durch Vollzeitbeschäftigte mit juristischer und technischer Sachkenntnis.
- Freigabe und Veröffentlichung von G10-Beschlüssen (vor allem derjenigen, die neue Rechts- und Technologiefragen betreffen);
- Veröffentlichung der Auslegung der Regierung bezüglich ihrer im Rahmen von Schlüsselgesetzen bestehenden gesetzlichen Befugnisse, der Grundsätze für die Überwachungspolitik und des Zwecks und der verfahrensmäßigen Einschränkungen von Überwachungsaktionen;
- Stärkung der parlamentarischen Aufsicht durch professionelles Personal, das sowohl über juristische als auch über technische Sachkenntnis verfügt und die uneingeschränkte Vollmacht hat, Dateien und laufende Programme für den Aufsichtsausschuss zu untersuchen;

Richtlinien, die neue allgemeine Genehmigungsstandards setzen, betriebliche Praktiken durch stärkere Schutzmaßnahmen für die Privatsphäre einschränken und die Transparenz erhöhen, sind Schritte in die richtige Richtung. Die Behandlung des Diskriminierungsproblems wird ein zentraler Punkt einer solchen Reformanstrengung sein. Letztendlich sorgen sich die Deutschen am meisten um die Verletzungen ihrer eigenen Privatsphäre durch ausländische Geheimdienste. Somit wird Deutschland, wenn es den Abstand zwischen den Persönlichkeitsrechten seiner eigenen Bürger und Ausländern deutlich verkleinert, in einer stärkeren Position sein, um bei engen Verbündeten und Partnern einschließlich der USA eine gleichartige Behandlung einzufordern.

Die US-Regierung hat begonnen, sich mit dem Diskriminierungsproblem zu befassen. In der PPD 28 heißt es, Nicht-US-Personen erhalten „im größtmöglichen Umfang, der mit der nationalen Sicherheit vereinbar ist“ den gleichen Schutz wie US-Bürger. Das ist die Grundlinie. Die PPD 28 garantiert Ausländern nicht dieselben Rechte und Schutzmaßnahmen wie US-Personen. Aber die US-Regierung hat die Gleichbehandlung als wichtiges Prinzip erkannt, dem die betrieblichen Praktiken der Erfassung auslandsnachrichtendienstlicher Informationen verpflichtet sein sollten. Nach meiner Kenntnis hat keine

---

[74] Matthias Bäcker, "Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes", *Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses*, 22. Mai 2014, https://www.bundestag.de/blob/280844/35ec929cf03c4f60bc70fc8ef404c5cc/mat a sv-2- 3-pdf-data.pdf

[75] Markus Löning, "Eine Reformagenda für die deutschen Geheimdienste: rechtsstaatlich, demokratisch, effektiv", stiftung neue verantwortung, 15. April 2015, http://www.stiftung-nv.de/publikation/eine- reformagenda-f%C3%BCr-die-deutschen-geheimdienste

andere Regierung ein vergleichbares Dokument veröffentlicht, das sich mit der Frage beschäftigt, welche Art von Richtlinien und Normen die Erfassung, Analyse, Speicherung und Verbreitung der Daten von Ausländern beschränkt.

Es überrascht nicht, dass Regierungen weltweit sich sträuben, das Diskriminierungsproblem anzupacken. Liberale Demokratien haben normalerweise gute gesetzliche Rahmenwerke für die Genehmigung, Durchführung und Beaufsichtigung der Überwachung im Hinblick auf ihre eigenen Bürger. Die Ausdehnung dieser gesetzlichen Rahmenwerke auf Geheimdienstaktionen, die Ausländer als Zielpersonen haben, würde den Schutz der Privatsphäre dieser Ausländer stark verbessern, die Geheimdienststellen aber auch dazu zwingen, einen sehr viel stärker zielgerichteten Ansatz in der Informationserfassung anzuwenden. Das könnte starke Einschränkungen für die Analyse, Speicherung und Verbreitung erfasster Daten mit sich bringen, was aber nicht bedeutet, dass es nicht getan werden könnte. Und viele Kritiker der aktuellen Geheimdienstpraktiken argumentieren, dass es sich günstig auswirken würde, wenn die Informationserfassung einen stärker strategischen und gezielten Ansatz verwenden würde, anstatt immer größere Heuhaufen anzusammeln in der Hoffnung, irgendwann die Nadeln zu finden.

Die Arbeit dieses Ausschusses hat Deutschland in eine starke Position gebracht, das erste Land zu sein, das die in den letzten zwei Jahren von den USA eingeführten Richtlinien und Normen übertrifft.
In ihrer ersten öffentlichen Anhörung erklärten prominente Verfassungsrechtsexperten, dass die deutsche Verfassung der deutschen Regierung vorschreibt, den in der Verfassung verankerten Schutz der Privatheit von Kommunikationen (Artikel 10) nicht nur in Deutschland und bei deutschen Bürgern, sondern darüber hinaus bei jedem Ausländer anzuwenden, der von der Überwachung durch deutsche Behörden betroffen ist.[76] Viele Parlamentarier und Regierungsbeamte, auch der deutsche Justizminister, haben öffentlich erklärt, dass das gesetzliche Rahmenwerk und die Beaufsichtigung des BND einer größeren Revision bedürfen.[77]

Vor einigen Wochen kündigte die Sozialdemokratische Partei (SPD) einen größeren Schritt nach vorn in der Behandlung des Diskriminierungsproblems an. Die SPD stellte ein Konzeptpapier vor, in dem die verfassungsrechtlichen Verpflichtungen nach Artikel 10 anerkannt werden und die Ausdehnung der Anwendbarkeit des G10-Gesetzes auf alle Überwachungsprogramme – nicht nur diejenigen, bei denen eine der Kommunikationslinien in Deutschland beginnt oder endet – gefordert wird.[78] Die Verfassungsreformen, die notwendig sind, um dieses Ziel zu erreichen – einschließlich der Erweiterung der Kapazitäten der G10-Kommission zur Überprüfung von Anträgen auf Überwachungsgenehmigungen – würden die Möglichkeit eröffnen, klare Standards für betriebliche Beschränkungen, Transparenz und Aufsicht zu setzen. Mit diesem Vorschlag als Reformgrundlage würde Deutschland international einen neuen Standard setzen und die Aufmerksamkeit auf neue Ideen zur Modernisierung der Datenschutz- und Sicherheitspolitik in demokratischen Gesellschaften lenken.

---

[76] Siehe Fußnote 74; Hans-Jürgen Papier, “Gutachtliche Stellungnahme”, *Beweisbeschluss SV-2 des ersten Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode,* 16. Mai 2014, https://www.bundestag.de/blob/280842/9f755b0c53866c7a95c38428e262ae98/mat a sv-2-2-pdf- data.pdf

[77] Jochen Gaugele, “BND einer demokratischen Kontrolle unterwerfen”, *Die Welt,* 17. Mai 2015, http://www.welt.de/politik/deutschland/article141009902/BND-einer-demokratischen-Kontrolle-unterwerfen.html

[78] SPD Bundestagsfraktion, “Eckpunkte der SPD-Bundestagsfraktion für eine grundlegende Reform der Strategischen Fernmeldeaufklärung des BND mit internationaler Vorbildwirkung”, 16. Juni 2015, http://www.spdfraktion.de/sites/default/files/2015-06-16-eckpunkte reform strafma-r-endfassung.pdf

Deutschland und die USA verfolgen in dieser Hinsicht ähnliche Projekte – die Schaffung von Gesetzen, die nicht nur für den Schutz von Privatsphäre und Sicherheit für die Nation angemessen sind, sondern auch in den Augen der Öffentlichkeit im In- und Ausland als legitim angesehen werden. Hierzu ist es erforderlich, demokratische Prinzipien für die Begrenzung der Macht der digitalen Überwachung durch ordentliche Gerichtsverfahren einzuführen. Dies erfordert Transparenz in den Genehmigungs- und Betriebsprozessen. Und es wird eine starke Aufsicht und Rechenschaftspflicht notwendig sein, um eine skeptische Öffentlichkeit davon zu überzeugen, dass die Anwendung der Macht in der digitalen Welt einer effektiven Kontrolle unterliegt.

Die Regierung Obama hat eine sorgfältige Prüfung ihrer Richtlinien und Praktiken vorgenommen, Reformen durchgeführt und einen neuen globalen Standard für transparente Politik hinsichtlich der Erfassung auslandsnachrichtendienstlicher Informationen gesetzt. Das sind bedeutende Schritte zur Wiederherstellung der Legitimität, und in dieser Hinsicht muss noch viel geschehen. Aber es ist unwahrscheinlich, dass Amerika diesen Weg alleine geht. Es wird einen Partner wie Deutschland brauchen, der sowohl Führerschaft als auch Partnerschaft zeigt. Die Angleichung von Sichtweisen und Praktiken zwischen unseren zwei Ländern wäre eine starke Botschaft an die internationale Gemeinschaft, denn wir gehen von sehr unterschiedlichen Ausgangspunkten an die Fragen der Privatsphäre und der Sicherheit heran.

Um die Position der NSA in der politischen Kultur Amerikas zu verstehen, ist es notwendig, die Idee des amerikanischen Exzeptionalismus zu verstehen. Einfach ausgedrückt, der amerikanische Nationalismus zelebriert seine eigene militärische Macht. Nach 9/11 wurde dieses Gefühl noch stärker, da die Regierung sich mit der Maximierung der Fähigkeiten harter Macht befasste. Das bedeutet, dass die Militär- und die Geheimdienstbehörden sich einer relativ unkritischen öffentlichen Unterstützung erfreuen – selbst wenn sie sich schlecht benehmen. Man bedenke, wie Militär und Spionage in der Popkultur dargestellt werden. Die NSA genießt nicht den gehobenen Status von Seal Team 6, gehört aber zu demselben politischen Zeitgeist. Und auch wenn viele Amerikaner wegen des ausgedehnten Systems der Überwachung durch die NSA beunruhigt sind, sind andere stolz darauf, dass wir bei dem, was wir tun, die besten sind. Und einige Amerikaner passen trotz des Widerspruchs in beide Kategorien.

Jetzt zum „deutschen Exzeptionalismus“. Der deutsche Nationalismus ist in Bezug auf militärische Macht eine Art Anti-Nationalismus – aus verständlichen Gründen. Das geht auf die Erfahrung zurück, dass Demokratie nicht notwendigerweise eine selbstkorrigierende Regierungsform ist. Oder einfacher ausgedrückt, die illegitime Nutzung von Macht kann zu unkontrollierter Radikalität führen. Die von der NSA ausgeübte Macht wäre ein Rezept für noch schlimmere Schrecken in der Geschichte des 20. Jahrhunderts gewesen. Deshalb ist ein Engagement zur Beschränkung der harten Macht des Staates tief in der deutschen Nachkriegsidentität verwurzelt. Nach meiner Meinung ist dies der Grund dafür, dass Deutschland – im Gegensatz zu fast allen anderen Ländern weltweit – die Snowden-Geschichte nicht einfach übergehen kann.

Darin liegt das Problem – dramatisch ausgedrückt: Die Amerikaner sehen die Macht der Geheimdienstbehörden als Ausdruck des amerikanischen Exzeptionalismus, und die Deutschen sehen die Kontrolle dieser Macht als Ausdruck ihres eigenen Exzeptionalismus. Wir müssen die Reformdebatte und die Aussichten für einen langfristigen Wandel vor dem Hintergrund dieser unterschiedlichen politischen Kulturen sehen. In diesem Zusammenhang ist es nicht überraschend, dass anfängliche Reformanstrengungen in Washington eher moderat ausfallen, während die Reaktion der deutschen Öffentlichkeit auf die NSA-Debatte in nachhaltiger Empörung besteht. Was überrascht, ist, dass eine gleichzeitige Reformagenda in Deutschland bisher keine ernsthafte Beachtung fand. Dieser Vergleich ist keine Entschuldigung für die Bescheidenheit der amerikanischen Reformen gegenüber der Mächtigkeit ihrer Aufklärungsaktionen. Solange jedoch andere nationale Reformanstrengungen fehlen, hat Amerika

den Maßstab für gesetzliche Beschränkungen und Transparenz gesetzt. Und dies führt unweigerlich zu folgendem Schluss: Wenn die amerikanische Bilanz bescheidener Reformen den globalen Standard setzt (was der Fall ist), kann keine Nation, die nicht selbst diesen Standard verbessert, von Washington glaubhaft mehr verlangen.

Diese Analyse der amerikanischen Reformanstrengungen zeigt, dass in den demokratischen Gesellschaften Spielraum für eine Führungsrolle in der Aufgabe vorhanden ist, alle unsere Annahmen über Sicherheit und Freiheit in Frage zu stellen. Dieser Untersuchungsausschuss hat in dieser Hinsicht Außerordentliches geleistet. Wenn die Tiefe und Intensität dieser Untersuchungen zu einer entsprechenden Reformagenda führen, wird Deutschland in der Modernisierung der Datenschutz- und Sicherheitspolitik in der digitalen Welt weltweit führend sein. Diese Errungenschaft wird ein Pluspunkt für die Prinzipien der deutschen Öffentlichkeit und ein wichtiger Beitrag für die langfristige Stabilität und moralische Autorität der transatlantischen Allianz sein.

Anhang: Offizielle Dokumente der US-Regierung zur Überwachungsreform

Gesetze, Richtlinien und Anordnungen

PATRIOT Act

- H.R. 3162, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001" http://frwebgate.access.gpo.gov/cgi- bin/getdoc.cgi?dbname=107 cong bills&docid=f:h3162enr.txt.pdf
- US Court of Appeals for The Second Circuit, Ruling regarding Section 215 (USA PATRIOT Act) http://www.ca2.uscourts.gov/decisions/isysquery/5b758b27-c77d-44a2-b6e5-dbf456f5c142/1/doc/14-42 complete opn.pdf

Foreign Intelligence Surveillance Act (FISA)

- Public Law 95-511, "Foreign Intelligence Surveillance Act of 1978", http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf

USA Freedom Act

- H.R.2048 - USA FREEDOM Act of 2015, Public Law No: 114-23 (06/02/2015) https://www.congress.gov/bill/114th-congress/house-bill/2048/text

Judicial Redress Act

- H.R.1428 - Judicial Redress Act of 2015, Vorlage im Repräsentantenhaus 18. März 2015 https://www.congress.gov/bill/114th-congress/house-bill/1428

Presidential Policy Directive - Signals Intelligence Activities (PPD-28)

- White House Press Release and Policy Directive https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive- signals-intelligence-activities
- Office of the Director of National Intelligence, "2015 Anniversary Report", 3. Februar 2015 http://icontherecord.tumblr.com/ppd-28/2015/overview

Executive Order 12333

- United States Intelligence Activities, Federal Register Vol. 40, No. 235 (December 8, 1981), amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008) http://www.dni.gov/index.php/about/organization/ic-legal-reference-book-2012/ref-book- eo-12333

Berichte

The President's Review Group on Intelligence and Communications Technologies

- Report: Liberty and Security in a Changing World, 12. Dezember 2013
  https://www.whitehouse.gov/sites/default/files/docs/2013-12-12 rg final report.pdf

Privacy and Civil Liberties Oversight Board

- Document Library: https://www.pclob.gov/library.html
- Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court
  https://www.pclob.gov/library/215-Report on the Telephone Records Program.pdf
- Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act https://www.pclob.gov/library/702-Report.pdf
- Recommendation Assessment Report
  https://www.pclob.gov/library/Recommendations Assessment-Report.pdf
  https://www.pclob.gov/library/Recommendations Assessment-FactSheet.pdf

National Academy of Sciences / National Research Council

- National Research Council, "Bulk Collection of Signals Intelligence: Technical Options", 15. Januar 2015,
  http://www.nap.edu/openbook.php7record id=19414

Freigegebene Dokumente

- Release of Documents Concerning Activities under the Foreign Intelligence Surveillance Act,
  http://icontherecord.tumblr.com/post/112610953998/release-of-documents- concerning-activities-under
- US Foreign Intelligence Surveillance Court, Docket Number 702(i)-08-01, Memorandum Opinion, 4. September 2008,
  http://www.dni.gov/files/documents/0315/FISC%200pinion%20September%204%202008.pdf
- U.S. Foreign Intelligence Surveillance Court, "Minimization Procedures used by NSA in Connection with FISA Section 702", 31. Oktober 2011
  https://www.aclu.org/sites/default/files/field_document/minimization_procedures_used_b_y_nsa in connection with fisa sect 702.pdf
- National Security Agency, "Overview of Signals Intelligence Authorities", 19. September 2014,
  https://www.aclu.org/files/assets/eo12333/NSA/0verview%20of%20Signals%20Intelligence%20Authorities.pdf
- Eine Liste der freigegebenen FISC-Gutachten befindet sich auch unter
  https://epic.org/privacy/surveillance/fisa/fisc/#orders