18. Wahlperiode

Deutscher Bundestag
1. Untersuchungsausschuss
nach Artikel 44 des Grundgesetzes

Stenografisches Protokoll
der 108. Sitzung
- endgültige Fassung* -

1. Untersuchungsausschuss
Berlin, den 8. September 2016, 11.30 Uhr
Paul-Löbe-Haus, Europasaal (4.900)
10557 Berlin, Konrad-Adenauer-Str. 1

Vorsitz: Prof. Dr. Patrick Sensburg, MdB

Tagesordnung - Öffentliche Beweisaufnahme

Tagesordnungspunkt

Öffentliche Anhörung von Sachverständigen

- Timothy H. Edgar, Watson Institute
- Ashley Gorski, ACLU, National Security Project
- Dr. Morton H. Halperin, Open Society Foundations
- Dr. Christopher Soghoian, ACLU, Principal Technologist
- Amie Stepanovich, Access Now, U.S. Policy Manager

_____
* Hinweis:
Die Korrekturen und Anmerkungen der Sachverständigen Amie Stepanovich sind im Protokoll eingefügt. (siehe Anlage 1) Die Sachverständigen Edgar, Gorski, Halperin und Soghoin haben keine Korrekturen übermittelt.

Mitglieder des Ausschusses

	Ordentliche Mitglieder	**Stellvertretende Mitglieder**
CDU/CSU	Sensburg, Prof. Dr. Patrick Lindholz, Andrea Schipanski, Tankred Warken, Nina	Marschall, Matern von Ostermann, Tim, Dr. Wendt, Marian
SPD	Flisek, Christian Mittag, Susanne	Zimmermann, Jens, Dr.
DIE LINKE.	Renner, Martina	Hahn, André, Dr.
BÜNDNIS 90/DIE GRÜNEN	Notz, Dr. Konstantin von	Ströbele, Hans-Christian

Fraktionsmitarbeiter

CDU/CSU	Feser, Andreas, Dr. Bredow, Lippold von Fischer, Sebastian D. Kordon, David Puglisi, Livia Schrot, Jacob Allers, Fried-Heye
SPD	Heyer, Christian Ahlefeldt, Johannes von Dähne, Dr. Harald Etzkorn, Irene Hanke, Christian-Diego Haupt, Philip Kilimann, Cecilia Weiß, Benjamin
DIE LINKE.	Halbroth, Anneke
BÜNDNIS 90/DIE GRÜNEN	Kant, Martina Leopold, Nils Pohl, Jörn

Beauftragte von Mitgliedern der Bundesregierung

Bundeskanzleramt	Jipp, Daniel Heinemann, Martin Kämmerer, Marie Pachabeyan, Maria Wolff, Philipp
Auswärtiges Amt	Berkemeier, Gunnar
Bundesministerium des Innern	Akmann, Torsten Beyer-Pollok, Markus Brandt, Dr. Karsten Darge, Dr. Tobias Matthes, Thomas Meyer, Till Weiss, Jochen
Bundesministerium für Wirtschaft und Energie	Scholl, Kirsten, Dr.
Bundesministerium für Verteidigung	Rauch, Rüdiger Theis, Björn

Original

(Beginn: 12.25 Uhr)

Vorsitzender Dr. Patrick Sensburg: Ich eröffne die 108. Sitzung des 1. Untersuchungsausschusses der 18. Wahlperiode.

Ich stelle fest: Die Öffentlichkeit ist hergestellt. Die Öffentlichkeit, die Vertreter der Presse und der Medien darf ich an dieser Stelle wieder ganz herzlich begrüßen.

Bevor ich zum eigentlichen Gegenstand der heutigen Sitzung komme, gestatten Sie mir einige Vorbemerkungen.

Ton- und Bildaufnahmen sind während der öffentlichen Beweisaufnahme grundsätzlich nicht zulässig; die meisten, die hier regelmäßig sind, kennen das. Wegen des besonderen öffentlichen Interesses hat der Ausschuss nach § 13 des Untersuchungsausschussgesetzes beschlossen, von der heutigen Sitzung ausnahmsweise eine Videoaufzeichnung durch die Bundestagsverwaltung fertigen zu lassen. Diese wird im Hauskanal des Deutschen Bundestages live übertragen. Sonstige Bild-, Ton- und Filmaufnahmen sind wie immer nicht zulässig. Entsprechende Geräte müssen leider abgeschaltet werden. Und, ich glaube, die Bundestagsverwaltung macht das in so einer exzellenten Qualität, dass wir dementsprechend auch eine gute Übertragung von dieser hochinteressanten Sitzung bekommen werden.

Ein Verstoß gegen dieses Gebot, Ton- und Bildaufnahmen während der Ausschusssitzung zu machen, kann nach dem Hausrecht des Bundestages nicht nur zu einem dauerhaften Ausschluss von den Sitzungen dieses Ausschusses sowie des ganzen Hauses führen, sondern gegebenenfalls auch strafrechtliche Konsequenzen nach sich ziehen. Ich bitte also darum, dem Ausschuss einen ungestörten Verlauf zu ermöglichen.

Ich rufe den **einzigen Punkt der Tagesordnung** auf:

Deutsche Übersetzung

Original

Öffentliche Anhörung von Sachverständigen

- Timothy H. Edgar, Watson Institute
- Ashley Gorski, ACLU, National Security Project
- Dr. Morton H. Halperin, Open Society Foundations
- Dr. Christopher Soghoian, ACLU, Principal Technologist
- Amie Stepanovich, Access Now, U.S. Policy Manager

Heute findet die öffentliche Beweisaufnahme aufgrund des Beweisbeschlusses SV-015 und des Beweisbeschlusses SV-016 statt. Es wird Beweis erhoben zum Untersuchungsauftrag - Bundestagsdrucksache 18/843 - durch Anhörung von Sachverständigen aus den Vereinigten Staaten. Die Anhörung findet ausschließlich öffentlich statt.

An dieser Stelle darf ich unsere Sachverständigen herzlich begrüßen, der Reihenfolge nach: Herrn Timothy Edgar vom Watson Institute, Frau Ashley Gorski, Anwältin bei ACLU, National Security Project, Herrn Morton Halperin, Senior Advisor der Open Society Foundations und ehemaliger Direktor von U.S. Advocacy, Herrn Chris Soghoian, technischer Experte bei ACLU, und Amie Stepanovich, Autorin bei Access Now und U.S. Policy Manager.

Herzlichen Dank, dass Sie heute hier sind, dass Sie unserer Einladung gefolgt sind und den weiten Weg auf sich genommen haben und dem Ausschuss heute für diese Anhörung zur Verfügung stehen. Es ist ja der einzige parlamentarische Untersuchungsausschuss, der sich mit dieser Thematik beschäftigt, und von daher freue ich mich sehr, dass Sie uns die Gelegenheit geben, doch einen viel deutlicheren und inneren Einblick in die Situation mit Blick auf die Vereinigten Staaten heute werfen zu können.

Deutsche Übersetzung

Original

Ich habe Sie darauf hinzuweisen, dass die Bundestagsverwaltung nicht nur eine Video-Liveübertragung anfertigt, sondern auch eine Tonaufnahme dieser Sitzung. Diese dient ausschließlich dem Zweck, die stenografische Aufzeichnung der Sitzung zu erleichtern. Diese Tonaufnahme, wird nach Erstellung des Protokolls dann gelöscht. Sie sehen ja auch unsere Stenografen - von Ihnen aus gesehen auf der rechten Seite -, die dann eben dementsprechend ein Protokoll anfertigen, und da ist die Tonbandaufnahme noch mal eine ergänzende Hilfe.

Das Protokoll dieser Anhörung wird Ihnen nach Fertigstellung zugestellt. Sie haben, falls dies gewünscht ist, dann die Möglichkeit, innerhalb von zwei Wochen Korrekturen und Ergänzungen vorzunehmen, falls etwas falsch aufgenommen worden ist oder falls Sie meinen, Korrekturen sind notwendig. - Gibt es hierzu Fragen von der Seite der Sachverständigen?

(Die Sachverständigen schütteln den Kopf)

Das ist gut. - Alle schütteln den Kopf. Dann habe ich zumindest eine kleine Gewissheit, dass die Übersetzung bei Ihnen ankommt. Okay.

Meine Damen und Herren Sachverständige, vor Ihrer Anhörung habe ich Sie als Sachverständige zu belehren. Sie sind als Sachverständige geladen worden. Als Sachverständige sind Sie ebenfalls verpflichtet, die Wahrheit zu sagen. Ihr Gutachten ist unparteiisch, nach bestem Wissen und Gewissen zu erstatten.

Ich habe Sie darauf hinzuweisen, dass es mögliche strafrechtliche Folgen haben kann, wenn gegen diese Wahrheitspflicht verstoßen wird. Wer vor dem Untersuchungsausschuss uneidlich falsch aussagt, kann gemäß § 162 in Verbindung mit § 153 des Strafgesetzbuches mit Freiheitsstrafen von drei Monaten bis zu fünf Jahren oder Geldstrafen bestraft werden.

Deutsche Übersetzung

Original

Nach § 28 in Verbindung mit § 22 Absatz 2 des Untersuchungsausschussgesetzes können Sie die Auskunft auf solche Fragen verweigern, deren Beantwortung Sie selbst oder Angehörige im Sinne des § 52 Absatz 1 der Strafprozessordnung der Gefahr aussetzen würde, einer Untersuchung nach einem gesetzlich geordneten Verfahren ausgesetzt zu werden. Dies betrifft theoretisch - bei Ihnen dürfte das bei allen fünfen nicht in Betracht kommen - auch Nebenverfahren bezüglich einer Straftat oder Ordnungswidrigkeit, auch Disziplinarverfahren; aber ich gehe davon aus, dass keiner von Ihnen in einem Beamtenverhältnis zu einer deutschen Behörde steht. - Gibt es hierzu Ihrerseits Fragen?

(Die Sachverständigen schütteln den Kopf)

Nein. Sehr gut. - Nach diesen notwendigen Vorbemerkungen darf ich Ihnen kurz den Ablauf der Untersuchungsausschusssitzung heute darstellen. Zu Beginn haben Sie nach § 28 in Verbindung mit § 24 Absatz 4 des Untersuchungsausschussgesetzes Gelegenheit, zum Beweisthema im Zusammenhang vorzutragen. Die Reihenfolge richtet sich nach dem Alphabet, also dementsprechend auch nach der Sitzordnung. Wir würden mit Herrn Edgar anfangen und dann von mir aus gesehen von links nach rechts alphabetisch weitergehen.

Sie haben die Möglichkeit, zu Anfang in einem sogenannten Eingangsstatement Ihre Sicht der Dinge - einige haben ja auch dementsprechend Gutachten bei uns abgegeben - zum Untersuchungsgegenstand innerhalb von 15 Minuten darzulegen. Also, wir haben uns vereinbart, dass ein Eingangsstatement Ihrerseits von jeweils 15 Minuten möglich ist. Ich hoffe, das ist für Sie ausreichend Zeit, um Ihre Sicht der Dinge darzulegen. So würden wir erst nacheinander die Eingangsstatements von Ihnen, sehr verehrte Sachverständige, hören und danach zu den Fragen der Mitglieder dieses Ausschusses kommen.

Es würde so sein, dass nach den Eingangsstatements dann die Fragen der Ausschussmitglieder

Deutsche Übersetzung

Original

kommen. Und wir haben uns darauf geeinigt, dass wir dies nicht nach einer Reihenfolge der Fraktionen machen oder nach festen Zeitkontingenten, sondern dass wir einfach nach der Reihenfolge der meldenden Kolleginnen und Kollegen die Fragen einzeln abarbeiten. Jeder Abgeordnete hat die Möglichkeit, Fragen zu stellen, nämlich zwei Fragen: entweder zwei Fragen an einen Sachverständigen oder an zwei Sachverständige jeweils eine Frage. Das ist das übliche Prozedere bei Sachverständigenanhörungen hier im Deutschen Bundestag. Und dann darf der nächste Kollege oder die nächste Kollegin hier aus diesem Kreis fragen. - Gibt es hierzu Nachfragen Ihrerseits zum Prozedere?

(Die Sachverständigen schütteln den Kopf)

Nein. - Dann sollten wir, glaube ich, loslegen. Ich würde gerne beginnen mit dem Eingangsstatement von Ihnen, Herr Edgar. Ich darf Ihnen das Wort geben für Ihre 15 Minuten. - Danke schön.

Sachverständiger Timothy H. Edgar: Thank you very much, Professor Dr. Patrick Sensburg and members of the committee. Thanks for the opportunity to testify on the topic of surveillance reform in the United States. We have made many reforms in the wake of the Snowden revelations and I just want to give you a few highlights of those in my written statement.

First I want to start out by reminding us that before a crowd of tens of thousands of Germans in the summer of 2008 we really saw an extraordinary scene of a young senator from Illinois, a candidate for President, Barack Obama, and he was promising a new spirit of cooperation in our foreign policy. When I looked back at that scene in preparation for this committee's hearing, I was really struck by his use of the word - - that we would look for allies who listen to each other, who learn from each other and who will,

Deutsche Übersetzung

Sachverständiger Timothy H. Edgar: *Ich danke Ihnen vielmals, Herr Professor Dr. Patrick Sensburg, und auch Ihnen, sehr geehrte Ausschussmitglieder. Vielen Dank für die Gelegenheit, heute hier zu Ihnen zum Thema der Überwachungsreform in den Vereinigten Staaten sprechen zu dürfen. Wir haben im Zuge der Snowden-Enthüllungen zahlreiche Reformen umgesetzt. Ich möchte Ihnen hierzu nur einige der wichtigsten aus meinem schriftlichen Gutachten vorstellen.*

Beginnen möchte ich jedoch mit einem Rückblick in den Sommer 2008, in dem wir erlebten, wie ein junger Senator aus Illinois, der Präsidentschaftskandidat Barack Obama, in einer außergewöhnlichen Rede vor Zehntausenden von Deutschen einen neuen Geist der Zusammenarbeit in unserer Außenpolitik versprach. Als ich mir diese Szene bei den Vorbereitungen für diese Ausschussanhörung in Erinnerung rief, stolperte ich förmlich über seine Worte - dass es uns um Verbündete geht, die einander zuhören,

Original

above all, trust each other. And, of course, the use of the word “listen” has a different context now after 2013.

Still, I think that we do want that kind of cooperative relationship, and so I welcome the opportunity to give the German parliament the experience that we have had since 2013 thanks to the Snowden revelations". And we’ve seen substantial reforms in intelligence practices. So, President Obama’s legacy will not simply be that of “the NSA scandal” as it’s called here or, as it’s called in the United States, “the Snowden revelations”, but will also be some of the bigger intelligence reforms when it comes to surveillance that we have seen, really, since the period of the mid-1970s, which my colleague Dr. Halperin can tell you about from personal experience.

My perspective on the issue of privacy and surveillance is shaped by my unique experience as well. From 2001 to 2006, I was the Legislative Counsel for national security for the American Civil Liberties Union, which is represented here, one of the largest and oldest non-governmental organizations in the world with a mission of defending fundamental rights. As an ACLU lawyer, I argued against many of the counterterrorism policies adopted by the administration of George W. Bush that we believed posed a threat to privacy and other civil liberties.

In early 2006, I had a unique opportunity, which was to go inside the intelligence community in a new office dedicated to safeguarding privacy and civil liberties. The Office of the Director of National Intelligence, which is the office that oversees all of the intelligence agencies in the United States, had created a new office inside that Office of the Director of National Intelligence called the Civil Liberties and Privacy Office. So, for the first time in American history, there would be a top advisor to the Director of

Deutsche Übersetzung

die voneinander lernen und die sich vor allem gegenseitig vertrauen. Die Wortwahl „zuhören“ hat nach 2013 natürlich eine ganz neue Dimension bekommen.

Dennoch denke ich, dass wir eine solche kooperative Beziehung wirklich wollen. Und deshalb begrüße ich die Gelegenheit, dem Deutschen Bundestag die Entwicklungen, die sich infolge der Snowden-Enthüllungen seit 2013 ergeben haben, schildern zu dürfen. Es hat grundlegende Reformen in der Arbeit der Geheimdienste gegeben. So wird das politische Erbe von Präsident Obama also nicht nur im „NSA-Skandal“, wie es in Deutschland heißt, oder auch in den „Snowden-Enthüllungen“, wie man in den USA sagt, bestehen, sondern auch in einigen der größten Reformen der geheimdienstlichen Überwachung seit Mitte der 1970er-Jahre, von denen Ihnen mein Kollege Dr. Halperin aus persönlicher Erfahrung erzählen kann.

Das Thema Datenschutz und Überwachung ist durch persönliche Erfahrungen geprägt. Von 2001 bis 2006 war ich als Legislative Counsel [Rechtsberater] für nationale Sicherheit der American Civil Liberties Union [ACLU; Amerikanische Bürgerrechtsunion], die hier vertreten ist, eine der größten und ältesten nichtstaatlichen Organisationen der Welt, die sich für Bürgerrechte einsetzt. Als Anwalt der ACLU habe ich mich gegen viele Terrorbekämpfungsmaßnahmen der Regierung von George W. Bush ausgesprochen, die wir als Gefahr für den Datenschutz und andere Grundrechte betrachteten.

Anfang 2006 ergab sich für mich eine einzigartige Gelegenheit, und zwar konnte ich in einer neuen Abteilung innerhalb des Geheimdienstes arbeiten, die sich dem Schutz der Privatsphäre und der Bürgerrechte widmen sollte. Das Büro des Director of National Intelligence, das sämtliche Geheimdienste der USA beaufsichtigt, hatte eine neue Dienststelle in ebendiesem Büro des Director of National Intelligence mit dem Namen Civil Liberties and Privacy Office [Büro für Bürgerrechte und Privatsphäre] geschaffen.

Original

National Intelligence, the head of the intelligence community, looking just at these issues of privacy and civil liberties. And they offered me a job to go in and work as the deputy in that office.

And when I came inside this office, I really was shocked and surprised by the breadth of NSA surveillance activities. Certainly, we knew that they had broad authorities, so we had made the case in the ACLU for the need for oversight of intelligence agencies. And yet the ways in which our intelligence agencies were using some of the new laws like the Patriot Act, they exceeded the kinds of things that I'd imagined as a civil liberties advocate in the ACLU: bulk collection, mass surveillance, these kinds of activities, which we hadn't even really anticipated in making the criticisms that we had of the sections of the Patriot Act that were being used in this way.

At the same time, I was somewhat surprised by how seriously everyone inside the government took the rules that governed intelligence surveillance. They may have interpreted these rules and stretched them well beyond what I had expected as a civil liberties lawyer, but they were very intent on ensuring that they adhered to those rules that they had. And what really was going on was not so much a clash between an out-of-control intelligence establishment that didn't want to obey the law or an intelligence establishment that was simply doing everything that they could to keep us safe, they were doing what they could to keep us safe but under laws that were inadequate for the digital age.

And what I mean by that is that the rules that governed intelligence surveillance, rules that most of the people I've met - all of the people actually, without exception - were intent on complying with, had simply been drafted for a

Deutsche Übersetzung

Zum ersten Mal in der amerikanischen Geschichte sollte es also einen hochrangigen Berater des Director of National Intelligence, des Leiters aller Geheimdienste, nur für die Themen Privatsphäre und Bürgerrechte geben. Und mir wurde die Position des Stellvertreters in diesem Amt angeboten.

Als ich meine Arbeit aufnahm, war ich wirklich schockiert und überrascht vom Ausmaß der Überwachungsaktivitäten der NSA. Sicherlich - wir wussten, dass die NSA weitreichende Vollmachten besaß, weswegen wir mit der ACLU ja auch die Aufsicht der Geheimdienste gefordert hatten. Und trotzdem gingen die Methoden, mit denen unsere Geheimdienste einige der neuen Gesetze wie den Patriot Act ausnutzten, über das hinaus, was ich mir als Bürgerrechtsanwalt in der ACLU hätte vorstellen können: massenhafte Datenerfassung, massenhafte Überwachung - Aktivitäten, die wir eigentlich gar nicht wirklich für möglich gehalten hatten, als wir die Passagen im Patriot Act kritisierten, die zu diesen Zwecken ausgenutzt wurden.

Gleichzeitig war ich doch recht überrascht davon, wie ernst jeder innerhalb der Regierung die Regeln nahm, denen die geheimdienstliche Überwachung unterlag. Diese Regeln wurden vielleicht weit über das, was ich als Bürgerrechtsanwalt erwartet hatte, hinaus ausgelegt und ausgedehnt; aber man war sehr darauf bedacht, die Regeln, die es gab, einzuhalten. Was eigentlich stattfand, war also nicht das Aufeinanderprallen zwischen einem außer Kontrolle geratenen Geheimdienstapparat, der dem Gesetz nicht gehorchen wollte, und einem Geheimdienstapparat, der einfach alles in seiner Macht stehende tat, um uns zu schützen; sie taten alles in ihrer Macht stehende, um uns zu schützen, aber unter Gesetzen, die dem Digitalzeitalter nicht gerecht wurden.

Was ich damit meine, ist, dass die Regeln für geheimdienstliche Überwachung, Regeln, auf deren Einhaltung die meisten Leute, die ich getroffen habe - eigentlich ausnahmslos alle Leute, die ich getroffen habe -, bedacht waren, schlicht und

Original

completely different period of time: a period before the Internet, a period before globalization, and a period before the rise of terrorism. And although these had been changed in certain ways to loosen them up after 9/11 to deal with the threat of terrorism, they had not been changed to deal with the threats to privacy that we've experienced as a result of the rise of the Internet.

We were intending in our office to engage in a dialogue with civil society over many of these changes. We had several meetings with my former group, with the ACLU, and others in order to engage in that kind of dialogue. But it was difficult to have that dialogue because of the demands of secrecy. It was hard for us to share with civil society the things that were really going on. These were classified activities. We could discuss in general ways the authorities that we had, but there's a big difference between discussing generally, "Here are some of the authorities that we have, and here are the ways in which they might be used", and saying, Here's what's really happening, let's talk about what to do to protect privacy.

A few days after I left government service to pursue my academic career at Brown University, a young government contractor, Edward Snowden, chose to reveal the details of two of the major programs on which I had worked - Prism and the bulk collection of telephone records - and then, over the next several months and now into years, has revealed many, many more details of programs that the NSA and other agencies have engaged in. And this decision precipitated an open debate on privacy and surveillance, the debate that we had wanted to have but never really were able to have. And that debate has forced significant changes to the way in which the United States government operates in the signals intelligence area. So I'll go through a few of those that are in my written statement.

Deutsche Übersetzung

einfach für eine andere Zeit gemacht worden waren: in einer Zeit vor dem Internet, einer Zeit vor der Globalisierung und einer Zeit vor der Ausbreitung des Terrorismus. Diese Regeln waren nach 9/11 zwar in bestimmter Weise geändert und gelockert worden, um den Gefahren des Terrorismus zu begegnen; sie waren aber nicht geändert worden, um den Gefahren zu begegnen, denen unsere Privatsphäre durch den Siegeszug des Internets ausgesetzt ist.

Unser Amt wollte mit der Zivilgesellschaft in einen Dialog treten, um über viele dieser Änderungen zu diskutieren. Wir sind mehrmals mit meiner ehemaligen Gruppe, der ACLU, und anderen zusammengekommen, um diesen Dialog anzustoßen. Doch die Geheimhaltungsanforderungen machten den Dialog schwierig. Was da wirklich passierte, ließ sich der Öffentlichkeit so kaum vermitteln. Die Aktivitäten waren Verschlusssache. Wir konnten allgemein über die Vollmachten sprechen, die wir hatten; aber es ist ein großer Unterschied, ob man ganz allgemein sagt: „Dies sind einige der Vollmachten, die wir haben, und mit denen könnten wir dieses oder jenes tun", oder ob man sagt: „Das ist das, was wirklich geschieht; lasst uns darüber reden, wie wir unsere Privatsphäre schützen können."

Ein paar Tage nachdem ich den Staatsdienst quittiert hatte, um meine akademische Laufbahn an der Brown University weiterzuverfolgen, enthüllte ein junger Auftragnehmer der Regierung namens Edward Snowden die Einzelheiten zu zwei der großen Programme, mit denen ich mich beschäftigt hatte - Prism und die massenhafte Erfassung von Telefonaufzeichnungen -, um dann, im Verlauf der nächsten Monate und mittlerweile Jahre, viele, viele weitere Einzelheiten zu Programmen zu enthüllen, die die NSA und andere Geheimdienste zum Einsatz gebracht haben. Mit diesem Schritt kam er einer offenen Debatte über Privatsphäre und Überwachung zuvor, also der Debatte, die wir führen wollten, aber nie wirklich konnten. Und diese Debatte hat grundlegende Änderungen in Bezug auf die Art und Weise, wie die US-amerikanische Regierung im Bereich der Signalaufklärung arbeitet,

Nur zur dienstlichen Verwendung

Original

The first one really is just the transparency. Obviously, there's transparency that came from the leaks that the government was forced to deal with, but instead of simply digging in its heels and saying, "These are leaks, and we don't comment on intelligence operations", under President Obama's leadership the intelligence community engaged in a major transparency drive to declassify thousands of pages of documents including documents from the once very secret Foreign Intelligence Surveillance Court. In fact, many of the revelations that we've talked about, especially those having to do with programs overseen by the FISA Court, have come from those documents rather than from the Snowden documents.

The second series of reforms has to do with the privacy of foreign citizens, citizens in Germany or anywhere else in the world. When I worked inside the intelligence community, there was no written policy or directive that I could point to say: This program has a massive impact on privacy around the world, of foreign citizens, it's not yielding very much intelligence, maybe we should scrap this program or change it. The only thing I could point to were directives and policies that had to do with the privacy of American citizens or permanent residents. So, you can look at these rules and you can say, "Well, there are holes or weaknesses" - and some of my colleagues have done that; I think that's a good exercise -, but I just want to pause for a minute and consider how important this change is that the world's largest intelligence power with some of its most important intelligence capabilities has made a policy statement written down in a way that it binds the intelligence communities that you do have to consider the privacy and civil liberties of everyone around the world and not

Deutsche Übersetzung

erzwungen. Ich werde also einige von denen skizzieren, die in meinem schriftlichen Gutachten erwähnt sind.

Die erste ist einfach nur die Transparenz. Natürlich stellten die Leaks, mit denen die Regierung sich gezwungenermaßen auseinandersetzen musste, an sich schon eine gewisse Transparenz her; aber anstatt einfach auf stur zu stellen und zu sagen: „Das sind Leaks, und wir kommentieren Geheimdienstoperationen nicht", machten sich die Geheimdienste unter der Führung von Präsident Obama daran, in einer großen Transparenzoffensive Tausende Dokumentseiten, unter anderem aus Dokumenten des einst sehr geheimen Foreign Intelligence Surveillance Court, freizugeben. Im Grunde stammen viele der Enthüllungen, über die gesprochen wurde, insbesondere jene, die mit Programmen zu tun haben, die durch den FISA Court [Gericht der Vereinigten Staaten betreffend die Überwachung der Auslandsaufklärung] überwacht wurden, aus diesen Dokumenten und nicht aus denen von Snowden.

Die zweite Serie von Reformen hat mit der Privatsphäre ausländischer Bürger zu tun, Bürger in Deutschland oder anderswo auf der Welt. Als ich innerhalb des Geheimdienstes tätig war, gab es keine schriftliche Richtlinie oder Vorschrift, die sich hätte heranziehen lassen, um zu sagen: Dieses Programm hat massive Auswirkungen auf die Privatsphäre ausländischer Bürger weltweit; es liefert nicht sehr viele Erkenntnisse; vielleicht sollten wir dieses Programm ausmustern oder ändern. - Das einzige, was sich heranziehen ließ, waren Richtlinien und Vorschriften, die mit der Privatsphäre von amerikanischen Staatsbürgern oder Aufenthaltsberechtigten zu tun hatten. Sie können sich diese Regeln nun ansehen und sagen: „Na gut, aber da gibt es Lücken und Schwächen." Und einige meiner Kollegen haben das gemacht - ich denke, das ist eine gute Übung. Aber ich möchte hier einfach einen Moment innehalten und überlegen, wie wichtig diese Entwicklung ist, dass das Land mit dem mächtigsten Geheimdienst der Welt und den größten Aufklärungsfähigkeiten der Welt eine

Original

just those of American citizens or residents. And I would suggest that this should lay down a marker for other countries, including Germany, to adopt similar policies, to say: Yes, we may have more restrictions for domestic surveillance and that's appropriate - we can get into why -, but we're not going to have no restrictions at all for external surveillance; we're going to have some level, some minimal level of understanding that the privacy of people outside our country does matter.

The other thing is that we have ended the bulk collection of American telephone records. That has less impact here in Germany, so I'll just say that it was an important debate inside the United States about the bulk collection idea.

The Foreign Intelligence Surveillance Court has opened itself up. There are now cleared lawyers who appear in front of it to argue the other side of issues that are important, where they used to only hear from government lawyers.

And then we can talk a little bit more also about the impact of the Schrems decision of the Court of Justice of the European Union, which has opened our intelligence services up to scrutiny by an international court and by international bodies, forcing us to justify why it is that we have certain types of practices. I think that that process is far from finished. I think that we in the United States are going to have to adopt additional reforms to address Schrems, and I think that's going to take many, many years.

Deutsche Übersetzung

Grundsatzerklärung niederschreibt, die seine Geheimdienste dazu verpflichtet, die Privatsphäre und Bürgerrechte von jedermann auf der Welt und nicht etwa nur von amerikanischen Staatsbürgern oder Einwohnern zu berücksichtigen. Und ich finde, dass dies auch für andere Länder, einschließlich Deutschland, den Anstoß liefern sollte, ähnliche Regeln einzuführen, zu sagen: „Ja, die inländische Überwachung unterliegt vielleicht stärkeren Beschränkungen und das ist angemessen - wir können gern darüber reden, warum -, aber wir werden keinesfalls gar keine Beschränkungen für eine ausländische Überwachung haben; wir werden ein gewisses Maß, ein Mindestmaß an Verständnis dafür haben, dass die Privatsphäre von Menschen außerhalb unseres Landes eine Rolle spielt."

Die andere Sache ist die, dass wir die massenhafte Erfassung amerikanischer Telefonaufzeichnungen eingestellt haben. Das ist für Deutschland weniger relevant. Deswegen sage ich hier lediglich, dass in den USA eine große Debatte über das Konzept der massenhaften Erfassung stattgefunden hat.

Der Foreign Intelligence Surveillance Court hat sich mittlerweile geöffnet. Vor ihm erscheinen jetzt zugelassene Anwälte, die in den wichtigen Fragen, zu denen früher nur die Anwälte der Regierung angehört wurden, die andere Seite vertreten.

Und dann können wir auch noch ein bisschen mehr über die Auswirkungen des Schrems-Urteils des Gerichtshofes der Europäischen Union sprechen, durch das unsere Geheimdienste ins Visier eines internationalen Gerichts und internationaler Organe gerieten und wir gezwungen waren, zu erklären, warum wir bestimmte Methoden anwenden. Ich denke, dieser Prozess ist noch lange nicht abgeschlossen. Ich glaube vielmehr, dass das Schrems-Urteil in den USA weitere Reformen notwendig macht. Und das wird noch viele, viele Jahre dauern.

Original

So I think this is a new reform era for intelligence surveillance in the United States. There is more to do. That era is not over. The Prism program and something called "Upstream collection" under Section 702 of the Foreign Intelligence Surveillance Act will come up for review next year in Congress, and we will have to decide whether to tighten up some of the provisions there. I think that they should be tightened up, specifically to address the Schrems decision and other concerns that have been expressed about the breadth of the surveillance under that authority.

I've written in a paper that I've submitted for the record a three-step process for how we could go about this next phase of intelligence reform. And my basic message here is that it's time to go big, to go global in intelligence reform. And that means that we should, in the United States, subject all of our mass surveillance programs under the NSA to judicial review by the Foreign Intelligence Surveillance Court, that we should have agreements with citizens of other democratic countries that we will limit the use of these extraordinary capabilities only to security threats and that we should provide a greater ability to challenge these kinds of surveillance programs in court. And here, I think, the United States could learn from the European practice in the case of Klass vs. Germany of essentially assuming that the surveillance is taking place in order to allow it to be tested in court rather than requiring people to show that they have actually been injured by surveillance, which is the rule in an American court and which frustrates the ability of ordinary federal courts to inquire into surveillance programs.

Deutsche Übersetzung

Ich denke also, wir befinden uns in den USA in einer neuen Phase der Reform der geheimdienstlichen Überwachung. Da gibt es noch einiges zu tun. Diese Phase ist noch nicht vorbei. Das Prism-Programm und die sogenannte „Upstream-Datenerfassung" nach § 702 des Foreign Intelligence Surveillance Act [FISA; Gesetz über Überwachungsmaßnahmen in der Auslandsaufklärung] wird im nächsten Jahr dem Kongress zur Überprüfung vorgelegt, und man wird entscheiden müssen, ob nicht einige der entsprechenden Bestimmungen verschärft werden sollten. Meiner Meinung nach sollten sie verschärft werden, insbesondere im Hinblick auf das Schrems-Urteil und andere Bedenken, die bezüglich des Ausmaßes der Überwachung unter dieser Vollmacht aufgekommen sind.

In einer von mir eingereichten Stellungnahme habe ich einen Drei-Schritte-Plan vorgeschlagen, wie sich diese nächste Phase der Geheimdienstreform in Angriff nehmen ließe. Ich vertrete darin die Ansicht, dass es an der Zeit ist, die Geheimdienstreform im großen Stil und weltweit voranzutreiben. Und das bedeutet, dass wir in den USA sämtliche Programme der NSA zur massenhaften Überwachung einer rechtlichen Überprüfung durch das Foreign Intelligence Surveillance Court unterstellen sollten, dass wir mit den Bürgern anderer demokratischer Länder vereinbaren sollten, die Nutzung dieser außergewöhnlichen Fähigkeiten auf Sicherheitsbedrohungen zu beschränken und dass mehr Möglichkeiten geschaffen werden, rechtlich gegen diese Arten von Überwachungsprogrammen vorzugehen. Hier können die USA meiner Meinung nach von der europäischen Verfahrensweise im Fall Klass gegen Deutschland lernen, und zwar dahin gehend, dass man die Tatsache, dass Überwachungsmaßnahmen stattfinden, voraussetzt, damit diese vor Gericht überprüft werden kann, anstatt von den Menschen den Nachweis zu verlangen, dass sie durch die Überwachung geschädigt wurden, was vor amerikanischen Gerichten die Regel ist und wodurch es ordentlichen Bundesgerichten unmöglich ist, Nachforschungen zu Überwachungsprogrammen anzustellen.

Original	*Deutsche Übersetzung*
So, with that I'll conclude my statement. Thank you very much for the opportunity to testify.	*Damit beende ich mein Statement. Ich danke Ihnen vielmals dafür, dass ich hier aussagen durfte.*
Vorsitzender Dr. Patrick Sensburg: Danke. Herzlichen Dank. - Ich freue mich nun über das nächste Eingangsstatement von Frau Gorski und würde Ihnen das Wort geben.	
Sachverständige Ashley Gorski: On behalf of the American Civil Liberties Union I would like to thank the committee of inquiry for holding this hearing and for the opportunity to testify on electronic surveillance conducted by the U.S. National Security Agency.	***Sachverständige Ashley Gorski:*** *Im Namen der American Civil Liberties Union [Amerikanische Bürgerrechtsunion] danke ich dem Untersuchungsausschuss für die Durchführung dieser Anhörung sowie für die Gelegenheit, zu den von der US-amerikanischen NSA durchgeführten elektronischen Überwachungsmaßnahmen aussagen zu dürfen.*
I'll begin today by speaking about three of the most significant lessons that we've learned from the Snowden disclosures. I'll then briefly discuss two major surveillance authorities: Section 702 of the Foreign Intelligence Surveillance Act, or FISA, and Executive Order 12333, which we refer to as "twelve-triple-three"; I don't know if that's much shorter, but that's the nomenclature. A more thorough discussion of these surveillance authorities is included in my written testimony, but I will present the abbreviated version here today. And I'll conclude by explaining why Presidential Policy Directive 28, otherwise known as PPD-28, one of the major post-Snowden surveillance reforms, does not go nearly far enough to curb in either Section 702 or EO 12333 surveillance.	*Beginnen werde ich meine Ausführungen mit drei der wichtigsten Lehren, die wir aus den Snowden-Enthüllungen gezogen haben. Anschließend spreche ich kurz über zwei zentrale Überwachungsvollmachten: § 702 des Foreign Intelligence Surveillance Act, kurz FISA, und die Executive Order EO 12333, die wir „Zwölf-Drei-Drei-Drei" nennen; ich weiß nicht, ob das viel kürzer ist, aber so ist die Nomenklatur. In meiner schriftlichen Stellungnahme gehe ich näher auf diese Überwachungsvollmachten ein; aber hier stelle ich heute die Kurzversion vor. Abschließend werde ich erklären, warum die Presidential Policy Directive 28, auch bekannt als PPD-28, als eine der zentralen Reformen der geheimdienstlichen Überwachung, die infolge der Snowden-Enthüllungen umgesetzt wurden, nicht annähernd ausreicht, um die Überwachungsmaßnahmen nach § 702 oder EO 12333 angemessen einzudämmen.*
Thanks to Edward Snowden and a group of particularly courageous reporters, over the past three years the U.S. public and elected officials have engaged in a long-overdue debate about government surveillance and civil liberties. This debate is ongoing and has been informed by three fundamental lessons about the nature of	*Dank Edward Snowden und einer Gruppe ausgesprochen mutiger Reporter haben die US-amerikanische Öffentlichkeit und Politik in den letzten drei Jahren eine seit langem überfällige Debatte über staatliche Überwachung und Bürgerrechte geführt. Grundlage dieser noch andauernden Debatte sind drei fundamentale Erkenntnisse über das Wesen der US-amerikanischen*

Original

U.S. surveillance and the legal and political structures in which it takes place.

First, through the Snowden disclosures and subsequent government revelations, the public is now aware that pervasive surveillance is not just theoretically possible, but it is in fact happening. Since the summer of 2013, we have learned, among other facts, that the NSA was collecting in bulk Americans' domestic phone records, that the NSA searches the content of substantially all text-based Internet communications that enter or exit the United States and that the NSA collects data outside of the United States on a massive scale, including emails, text messages, Internet chat transcripts, the full content of phone conversations, cell phone location information, and contact lists. For example, as reported by the press, the NSA collects and retains data from approximately 500 million German phone and Internet communications each month.

Second, we've learned that the U.S. lacks an adequate system of checks and balances to oversee and restrain executive-branch surveillance. When the government conducts surveillance that takes place on U.S. soil or targets Americans, a secret court, known as the Foreign Intelligence Surveillance Court or FISC, is supposed to serve as a check on the executive branch's surveillance activities. But it has become apparent that the secret court has failed to meaningfully constrain the executive branch. Even more problematically, when the U.S. conducts surveillance overseas, it is subject to very little congressional oversight and no judicial oversight despite the fact that this surveillance sweeps countless Americans into its dragnet. And, as my colleague mentioned, as a general matter, it is exceptionally difficult to challenge the government's surveillance programs in ordinary courts. Civil litigants are almost always stymied by the doctrine of "standing", which requires them to show with sufficient likelihood that they have been or will be subject to secret surveillance. In addition, the government has an

Deutsche Übersetzung

Überwachung und die rechtlichen und politischen Strukturen, in denen sie stattfindet.

Erstens ist der Öffentlichkeit durch die Snowden-Enthüllungen und anschließenden Offenlegungen der Regierung bewusst geworden, dass allgegenwärtige Überwachung nicht nur theoretisch möglich ist, sondern tatsächlich stattfindet. Seit dem Sommer 2013 haben wir zudem erfahren, dass die NSA massenhaft amerikanische Telefongespräche aufzeichnete, dass die NSA den Inhalt praktisch der gesamten textbasierten Internetkommunikation durchsucht, die in den USA empfangen oder von dort aus versendet wird, und dass die NSA auch außerhalb der USA im großen Stil Daten sammelt, darunter E-Mails, Textnachrichten, Internet-Chat-Protokolle, den gesamten Inhalt von Telefongesprächen, Positionsdaten von Mobiltelefonen und Kontaktlisten. Beispielsweise sammelt und speichert die NSA laut Presseberichten monatlich die Daten zu etwa 500 Millionen deutschen Telefon- und Internetkommunikationen.

Zweitens haben wir erfahren, dass die USA über kein hinreichendes gegenseitiges Kontrollsystem [Checks and Balances] verfügen, um die Überwachung von Organen der Exekutive zu beaufsichtigen und zu begrenzen. Im Falle von Überwachungen der Regierung auf US-amerikanischem Boden oder von Amerikanern ist ein geheimes Gericht, auch bekannt als der Foreign Intelligence Surveillance Court oder FISC, für die Kontrolle der Überwachungsaktivitäten gegenüber der Exekutive zuständig. Noch problematischer ist, dass Überwachungsaktivitäten der Regierung im Ausland nur in sehr geringem Umfang vom Kongress und überhaupt nicht von Gerichten kontrolliert werden, obwohl auch zahllose Amerikaner ins Schleppnetz dieser Überwachungen geraten. Zudem ist es, wie mein Kollege bereits sagte, grundsätzlich sehr schwierig, auf dem ordentlichen Rechtsweg gegen die Überwachungsprogramme der Regierung vorzugehen. Zivilklagen werden fast immer durch die Doctrine of „Standing" [Klagebefugnis-Doktrin] abgewürgt, die verlangt, dass der Kläger mit hinreichender Wahrscheinlichkeit nachweist, Ziel

Original

obligation to notify criminal defendants when it intends to use evidence against them that was obtained or derived from surveillance programs, and the government relies on a very narrow interpretation of its notice obligation. As a result, countless criminal defendants who have been subject to highly controversial surveillance programs are unable to challenge them in any court.

Third, the U.S. government is not sufficiently transparent about its interpretations of surveillance law and the scope of its practices. Indeed, in many respects, the Snowden disclosures themselves were the product of a culture of excessive secrecy. No one is suggesting that the U.S. should reveal every last operational detail related to its surveillance activities. But in order to maintain democratic legitimacy, the government must be more forthcoming with the public about the general scope of its surveillance as well as its understanding of the breadth of its legal authorities.

Informed by these three lessons, the debate over privacy and surveillance has resulted in some reforms, the most significant of which relates to the NSA's domestic call-records program. For more than a decade, the NSA kept a record of substantially all phone calls made or received on major U.S. telephone networks. The ACLU challenged the legality of this surveillance in court, and a federal court of appeals ruled in May 2015 that this bulk surveillance was illegal. Shortly thereafter, Congress passed the USA Freedom Act, which put an end to the NSA's bulk collection of domestic call records. While the passage of this act was a milestone, the legislation left many of the government's most intrusive and overbroad surveillance authorities untouched.

Deutsche Übersetzung

einer Überwachung zu sein oder gewesen zu sein. Darüber hinaus ist der Staat verpflichtet, einen Angeklagten in einem Strafverfahren darüber zu informieren, dass er Beweise gegen ihn verwenden will, die durch Überwachung erlangt oder daraus abgeleitet wurden. Der Staat legt diese Mitteilungspflicht jedoch sehr eng aus. Daher ist es unzähligen Angeklagten, die Ziel hochkontroverser Überwachungsprogramme geworden sind, nicht möglich, sich vor einem ordentlichen Gericht dagegen zur Wehr zu setzen.

Drittens legt die US-Regierung nicht transparent genug dar, wie sie die gesetzlichen Bestimmungen zur Überwachung auslegt und in welchem Umfang sie Überwachungen durchführt. Im Grunde waren die Snowden-Enthüllungen selbst das Ergebnis einer exzessiven Geheimhaltungskultur. Niemand verlangt, dass die US-Regierung ihre Überwachungsaktivitäten bis ins letzte Detail offenlegt. Damit die demokratische Legitimierung gewahrt bleibt, darf die Regierung der Öffentlichkeit jedoch nicht verheimlichen, in welchem allgemeinen Umfang sie Überwachung betreibt und wie weit die entsprechenden Vollmachten ihrem Verständnis nach reichen.

Auf Grundlage dieser drei Lehren hat die Debatte über Privatsphäre und Überwachung zu einigen Reformen geführt. Die wichtigste davon bezieht sich auf das NSA-Programm zur Aufzeichnung inländischer Telefongesprächsdaten. Über mehr als ein Jahrzehnt hinweg hat die NSA praktisch alle Telefonanrufe erfasst, die über die größten US-amerikanischen Telefonnetze getätigt bzw. angenommen wurden. Die ACLU ist gegen diese Überwachung vor Gericht gegangen, und im Mai 2015 hat ein Bundesberufungsgericht entschieden, dass diese massenhafte Überwachung rechtswidrig war. Kurz darauf erließ der Kongress den USA Freedom Act, der die massenhafte Erfassung inländischer Anrufdaten beendete. Auch wenn die Verabschiedung dieses Gesetzes einen Meilenstein darstellt, ließ die Gesetzgebung viele der Vollmachten unberührt, die besonders unverhältnismäßig sind und den Schutz der Privatsphäre am stärksten beeinträchtigen.

Original

Next, I'll briefly discuss two of those authorities: Section 702 of FISA, which authorizes surveillance that takes place on U.S. soil, and Executive Order 12333, which authorizes electronic surveillance that largely takes place abroad.

Section 702 authorizes the government's large-scale, warrantless acquisition of the contents of communications inside the U.S. when two primary conditions are satisfied: first, the target of the NSA's surveillance must be a foreigner located abroad and, second, the purpose of the surveillance must be to gather "foreign intelligence information". But, importantly, neither of these conditions imposes a meaningful restraint on the government's surveillance. Section 702 does not require the government to make any finding - let alone demonstrate a probable cause to a court - that its surveillance targets are foreign agents, engaged in criminal activity, or even remotely associated with terrorism. Additionally, the phrase "foreign intelligence" is defined extraordinarily broadly to include information related to the foreign affairs of the United States. Thus, the government's authority is not limited to the surveillance of suspected terrorists or criminals, but extends to the surveillance of individuals who are not suspected of any wrongdoing whatsoever.

The Snowden revelations and subsequent government disclosures show that the government uses Section 702 to conduct at least two types of surveillance: Prism and Upstream surveillance. Upstream involves the mass copying and searching of virtually all Internet communications flowing into and out of the United States. With the help of companies like Verizon and AT&T, the NSA conducts this surveillance by tapping directly into the Internet backbone in

Deutsche Übersetzung

Als nächstes werde ich kurz über zwei dieser Vollmachten sprechen: § 702 des FISA, wonach die Durchführung von Überwachungsmaßnahmen auf US-amerikanischem Boden zulässig ist, und EO 12333, wonach die überwiegend im Ausland stattfindende elektronische Überwachung zulässig ist.

Der § 702 bildet die Rechtsgrundlage für die weitreichende Beschaffung von Kommunikationsinhalten ohne richterlichen Beschluss innerhalb der USA, sofern zwei Voraussetzungen erfüllt sind: Erstens muss das von der NSA überwachte Ziel ausländischer Staatsbürger sein und sich im Ausland befinden, und zweitens muss der Zweck der Überwachung darin bestehen, „ausländische geheimdienstliche Informationen" zu sammeln. Wichtig ist hier jedoch, dass keine dieser beiden Bedingungen die Überwachung durch die Regierung in konkreter Weise beschränkt. Der § 702 verlangt von der Regierung keinerlei Ermittlungsergebnisse, geschweige denn das Vorbringen wahrscheinlicher Gründe gegenüber einem Gericht, dass die von ihr überwachten Ziele ausländische Agenten, in Straftaten verwickelt oder auch nur im Entferntesten mit Terrorismus in Verbindung zu bringen sind. Zudem ist der Begriff „ausländische geheimdienstliche Informationen" im Sinne von Informationen, die die Außenpolitik der USA betreffen, ausgesprochen weit gefasst. Somit beschränkt sich die Vollmacht der Regierung nicht auf die Überwachung von Verdachtspersonen, wie mögliche Terroristen oder Kriminelle, sondern erstreckt sich auch auf die Überwachung von Personen, die unter keinerlei Verdacht einer Straftat stehen.

Die Snowden-Enthüllungen und anschließenden Offenlegungen der Regierung zeigen, dass die Regierung sich bei zumindest zwei Arten der Überwachung auf § 702 stützt: Prism und Upstream-Überwachung. Upstream ist das massenhafte Kopieren und Durchsuchen praktisch aller Internetkommunikationen, die in die USA hinein- oder aus den USA hinausfließen. Mithilfe von Unternehmen wie Verizon und AT&T zapft die NSA bei dieser Art von Überwachung

Original

the U.S., the system of cables, switches and routers, the physical infrastructure that carries Americans' communications with each other and with the rest of the world. After copying nearly all of this traffic, the NSA searches both the metadata and the content for key terms, called "selectors", that are associated with its tens of thousands of foreign targets. We know that these selectors take the form of email addresses and phone numbers, for example. But that's not an exhaustive list. Communications containing selectors are retained on a longer-term basis for further analysis and dissemination, with few restrictions.

The second type of Section 702 surveillance is known as Prism. Through Prism, the government obtains communications directly from U.S.-based service providers such as Google, Yahoo, Microsoft and Facebook. The government identifies the user accounts it seeks to monitor, for example, particular Yahoo email addresses, and then it collects from the provider all communications to or from those accounts. As of April 2013, the NSA was monitoring at least 117,000 targeted accounts via Prism.

I'll now speak briefly about Executive Order 12333, which was originally issued in 1981 by President Reagan. It's the primary authority under which the NSA gathers foreign intelligence. It provides broad latitude for the government to surveil Americans and others alike without judicial review or other protections that apply to surveillance conducted under statutory authorities. Despite its breadth, EO 12333 has not been subject to meaningful oversight. Surveillance programs operated under the executive order have never been reviewed by any court. And, as the former chairman of the Senate Intelligence Committee has conceded, they are not overseen in a meaningful way by Congress. EO 12333 authorizes the government to conduct electronic

Deutsche Übersetzung

das Rückgrat des Internets in den USA an, also das System aus Kabeln, Verteilern und Routern, die physische Infrastruktur, über die alle Amerikaner untereinander und mit dem Rest der Welt kommunizieren. Die NSA kopiert nahezu den gesamten Datenverkehr und durchsucht anschließend sowohl die Metadaten als auch den Inhalt nach Schlüsselbegriffen, sogenannten „Selektoren", die eine Verbindung zu den Zehntausenden von ausländischen Zielen aufweisen. Wir wissen, dass diese Selektoren zum Beispiel aus E-Mail-Adressen und Telefonnummern bestehen können. Aber es gibt noch weitere. Kommunikationen, die Selektoren enthalten, werden ohne wesentliche Beschränkungen zur genaueren Analyse und zur Weitergabe langfristiger gespeichert.

Die zweite Art von Überwachung gemäß § 702 ist unter der Bezeichnung „Prism" bekannt. Mit Prism bezieht die Regierung die Kommunikationen unmittelbar von US-amerikanischen Providern wie Google, Yahoo, Microsoft und Facebook. Die Regierung identifiziert dann die gesuchten Nutzerkonten, um zum Beispiel bestimmte E-Mail-Adressen von Yahoo zu überwachen, und holt sich dann vom Provider die gesamte Kommunikation, die über diese Konten versendet oder empfangen wird. Im April 2013 betrug die Zahl der von der NSA via Prism überwachten Zielkonten 117 000.

Ich werde jetzt kurz auf die EO 12333 eingehen, die ursprünglich im Jahr 1981 von Präsident Reagan erlassen wurde. Dies ist die primäre Rechtsgrundlage, unter der die NSA geheimdienstliche Aufklärung im Ausland betreibt. Sie bietet der Regierung einen großen Spielraum für die Überwachung von Amerikanern und anderen Staatsbürgern ohne richterliche Kontrolle oder andere Schutzbestimmungen, die auf gesetzlich zugelassene Überwachungsmaßnahmen anwendbar sind. Trotz der weitreichenden Befugnisse unterliegt EO 12333 keiner nennenswerten Kontrolle. Überwachungsprogramme, die unter der Executive Order betrieben werden, sind noch nie gerichtlich überprüft worden. Und wie

Original

surveillance abroad for the purpose of collecting "foreign intelligence", and again, this term is defined extremely broadly, even more broadly than it's defined under Section 702. Essentially it likely permits surveillance of any foreign person.

In addition, the order and its implementing regulations permit two forms of bulk surveillance. First, they permit the government to engage in what is sometimes termed "bulk collection". That is the indiscriminate collection and retention of electronic communications or data. Second, the order and its implementing regulations allow what might be called "bulk searching", in which the government has access, on a generalized basis, to electronic communications, temporarily copies those communications, searches them for "selection terms", which aren't limited to email addresses and phone numbers, and retains for long-term use any communications containing those terms. This is the bulk searching that also happens under Section 702 of FISA, but in that context there are greater limitations on the nature of the selectors that are used.

So I'll now touch on the most significant aspects of PPD-28 and explain why these reforms are an important step in the right direction but do not go nearly far enough.

PPD-28 was issued in January 2014 by President Obama. It is an executive-branch directive that articulates broad principles to govern the collection of signals intelligence, and it imposes certain constraints on the use of electronic communications that were obtained in bulk and the retention and dissemination of communications

Deutsche Übersetzung

der ehemalige Vorsitzende des Senate Intelligence Committee einräumte, unterstehen sie keiner nennenswerten Kontrolle durch den Kongress. EO 12333 bevollmächtigt die Regierung zur Durchführung elektronischer Überwachungsmaßnahmen im Ausland zwecks Sammlung "ausländischer geheimdienstlicher Informationen", und auch hier ist dieser Begriff weit gefasst, und zwar sogar noch weiter als nach § 702. Im Prinzip genehmigt er wahrscheinlich die Überwachung jeder ausländischen Person.

Darüber hinaus erlauben die Executive Order und ihre Durchführungsverordnungen zwei Formen von massenhafter Überwachung. Erstens ermöglichen sie der Regierung die Praxis der sogenannten „massenhaften Erfassung". Hierunter versteht man die willkürliche Erfassung und Speicherung elektronischer Kommunikationen oder Daten. Zweitens erlauben die Executive Order und ihre Durchführungsverordnungen das sogenannte „massenhafte Durchsuchen", bei dem die Regierung den allgemeinen Zugang zu elektronischer Kommunikation erhält, diese Kommunikation vorübergehend kopiert, sie nach „Selektionsbegriffen", zu denen nicht nur E-Mail-Adressen und Telefonnummern gehören, durchsucht und schließlich die Kommunikation, in denen diese Begriffe enthalten sind, langfristig speichert. Dies ist die massenhafte Durchsuchung, die auch nach § 702 des FISA stattfindet, jedoch bestehen in diesem Zusammenhang größere Beschränkungen hinsichtlich der verwendeten Selektoren.

Ich komme jetzt also zu den wesentlichen Aspekten der PPD-28 und erkläre, warum diese Reformen ein wichtiger Schritt in die richtige Richtung sind, aber nicht annähernd weit genug gehen.

Die PPD-28 wurde im Januar 2014 von Präsident Obama erlassen. Es handelt sich dabei um eine Direktive der Exekutive, in der grobgefasste Prinzipien zur Reglementierung der Datenerfassung im Rahmen von Signalaufklärung formuliert sind. Die Direktive setzt gewisse Grenzen hin-

Original

containing personal information of non-U.S. persons. The ACLU applauds PPD-28's recognition of the privacy interests of non-U.S. persons. However, the directive includes few meaningful reforms, and these reforms can easily be modified or revoked by the next U.S. President. At bottom, PPD-28 is designed to accommodate the government's ongoing bulk surveillance of both U.S. and non-U.S. persons.

The directive provides that when the U.S. collects non-publicly available signals intelligence in bulk, it shall use that data only for the purposes of detecting and countering six specified activities, which I think Dr. Halperin may discuss in greater detail. One of these activities is potentially quite broad though, and that's transnational criminal threats. These restrictions are obviously a step in the right direction, but they do not go nearly far enough to constrain the collection of U.S. and non-U.S. person data. In essence, they effectively ratify the practice of bulk, indiscriminate surveillance for a variety of purposes despite the fact that bulk surveillance violates article 17 of the International Covenant on Civil and Political Rights and, separately, that such bulk surveillance is at odds with the CJEU's opinion in Schrems.

Moreover, PPD-28's limitations on bulk collection do not extend to other problematic types of mass surveillance including the bulk searching of Internet communications that I described earlier. In other words, these restrictions on use do not apply to data that is held for a short period of time and searched in bulk, such as the data

Deutsche Übersetzung

sichtlich der Verwendung von massenhaft beschaffter elektronischer Kommunikation und der Speicherung und Weitergabe von Kommunikationen, die personenbezogene Daten ausländischer Personen enthält. Die ACLU begrüßt, dass mit der PPD-28 die Datenschutzinteressen von Nicht-US-Personen Anerkennung finden. Jedoch enthält die Direktive wenig ernstzunehmende Reformen. Und diese Reformen lassen sich vom nächsten US-Präsidenten nur zu leicht ändern oder zurücknehmen. Unter dem Strich kommt die PPD-28 der fortlaufenden massenhaften Überwachung von sowohl US- Personen als auch Nicht-US- Personen durch die Regierung entgegen.

Die Direktive sieht Folgendes vor: Wenn die USA Signalaufklärung zur massenhaften Erfassung nicht öffentlich zu empfangender Daten betreiben, dürfen diese Daten ausschließlich zur Aufdeckung und Verhinderung von sechs bestimmten Aktivitäten, die Dr. Halperin, glaube ich, noch näher erläutern wird, verwendet werden. Eine dieser Aktivitäten ist allerdings potenziell ziemlich weit gefasst, und zwar die Bedrohung durch grenzüberschreitende Kriminalität. Diese Beschränkungen sind natürlich ein Schritt in die richtige Richtung; aber sie setzen der Erfassung personenbezogener Daten von US-Personen und Nicht-US-Personen nicht annähernd ausreichende Grenzen. Im Grunde segnen sie die Praxis der massenhaften, willkürlichen Überwachung für eine ganze Reihe von Zwecken ab, obwohl die massenhafte Überwachung gegen Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte verstößt und obwohl, davon abgesehen, eine solche massenhafte Überwachung der Auffassung des Gerichtshofs der Europäischen Union im Schrems-Urteil zuwiderläuft.

Außerdem erstrecken sich die in der PPD-28 formulierten Beschränkungen der massenhaften Erfassung nicht auf andere problematische Formen der massenhaften Überwachung, einschließlich des eingangs beschriebenen massenhaften Durchsuchens von Internetkommunika-

Original

that is held and searched in bulk through Upstream surveillance under Section 702.

PPD-28's most significant reforms are with respect to the retention and dissemination of communications containing personal information of non-U.S. persons. However, even these reforms do little to rein in the government's mass violations of the privacy rights of foreigners. Under the directive, the government may retain or disseminate the personal information of non-U.S. persons only if retention or dissemination of comparable information about U.S. persons would be permitted under EO 12333. Critically, however, EO 12333 imposes very few restraints on the government: it authorizes the retention and dissemination of communications to, from, and about U.S. persons when, just as an example, those communications contain "foreign intelligence," which, again, is defined extremely broadly. Thus, while the executive branch's efforts to create new protections for non-U.S. persons are welcome - and they are certainly long overdue -, these protections are extremely weak.

So, in conclusion, I'll just note that the Snowden disclosures and subsequent domestic debates over privacy have resulted in some surveillance reforms in the U.S. However, two of the most significant surveillance authorities, Section 702 and EO 12333, remain largely intact.

I'd like to thank you again for the invitation to discuss the legal frameworks governing U.S. foreign intelligence surveillance. The ACLU appreciates the committee of inquiry's attention to these issues.

Deutsche Übersetzung

tionen. Mit anderen Worten: Diese Beschränkungen bezüglich der Verwendung gelten nicht für Daten, die nur kurze Zeit gehalten und massenhaft durchsucht werden, wie zum Beispiel die im Rahmen der Upstream-Überwachung gemäß § 702 gehaltenen und massenhaft durchsuchten Daten.

Die wichtigsten in der PPD-28 enthaltenen Reformen beziehen sich auf die Speicherung und Weitergabe von Kommunikationen, die personenbezogene Daten von Nicht-US-Personen enthalten. Aber selbst diese Reformen wirken der massenhaften Verletzung des Rechts auf Privatsphäre ausländischer Bürger durch die Regierung kaum entgegen. Der Direktive zufolge darf die Regierung die personenbezogenen Daten von Nicht-US-Personen nur dann speichern oder weitergeben, wenn die Speicherung oder Weitergabe vergleichbarer Daten über US-Personen nach EO 12333 zulässig wäre. Unglücklicherweise sind die Beschränkungen, die der Regierung durch EO 12333 auferlegt werden, jedoch sehr gering: Es erlaubt die Speicherung und Weitergabe von Kommunikationen an, von und über US-Personen, wenn, nur als Beispiel, diese Kommunikation „ausländische geheimdienstliche Informationen" enthält, die wiederum einer sehr weitgefassten Definition unterliegen. Insofern sind die Bemühungen, neue Regeln zum Schutze von Nicht-US-Personen einzuführen zwar begrüßenswert - und sie sind sicherlich seit langem überfällig -, aber der Schutz ist extrem schwach.

Also möchte ich abschließend festhalten, dass die Snowden-Enthüllungen und anschließenden Debatten über Privatsphäre in den USA zu einigen Überwachungsreformen geführt haben. Dennoch bleiben zwei der wichtigsten Rechtsgrundlagen für Überwachung, § 702 und EO 12333, weitgehend unverändert bestehen.

Ich möchte mich nochmals dafür bedanken, dass ich hier heute zu Ihnen über den Rechtsrahmen der geheimdienstlichen Überwachungsaktivitäten der USA sprechen durfte. Die ACLU

Original

Thank you.

Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank für Ihre Ausführungen, Mrs. Gorski. - Als Nächsten hätten wir jetzt Herrn Halperin. Sie sind ja schon angesprochen worden. Ich darf das Wort direkt weitergeben an Sie für Ihre Einführungsausführungen. Danke schön.

Sachverständiger Dr. Morton H. Halperin: I join my colleagues in expressing appreciation for the opportunity to testify before this committee.

I think what I want to do is to focus my remarks on one aspect of the problem. I agree that the reforms in the United States since the Snowden revelations have been important, and I also agree that they don't go anywhere near far enough and that there is still a great deal to be done, even in terms of surveillance of American citizens within the United States. But I think, in some ways, the most important change that's taking place is the recognition in the American government for the first time that there is an obligation, a commitment, a need to respect the privacy of private citizens of other countries.

We can have a long argument about whether this is required by existing international legal obligations. We can have an argument about whether the American constitution applies or not. But I think the important fact is that as a matter of policy the American government has begun a dialogue which says: democratic governments owe respect to the privacy of private citizens, at least of other democratic countries. And I think there is a real opportunity, which I think depends on the cooperation between the Federal Republic and the United States, to pick up on that opening and to make a change, which would be a fundamental change, in the way

Deutsche Übersetzung

weiß zu schätzen, dass der Untersuchungsausschuss auf diese Problematik aufmerksam macht.

Vielen Dank.

Sachverständiger Dr. Morton H. Halperin: *Ebenso wie meine Kollegen möchte ich mich bei Ihnen ausdrücklich für die Gelegenheit, vor dem Ausschuss aussagen zu dürfen, bedanken.*

Ich denke, ich werde mich auf einen Aspekt des Problems konzentrieren. Ich bin ebenfalls der Meinung, dass die Reformen, die seit den Snowden-Enthüllungen in den USA umgesetzt wurden, wichtig sind. Und ich stimme zu, dass sie nicht annähernd weit genug gehen und dass es noch viel zu tun gibt, und zwar sogar auch in Bezug auf die Überwachung amerikanischer Staatsbürger in den USA. Aber ich denke, in gewisser Weise besteht die wichtigste der gerade stattfindenden Änderungen in der erstmaligen Einsicht der amerikanischen Regierung, dass es eine Pflicht, eine Verpflichtung, eine Notwendigkeit gibt, die Privatsphäre von Bürgern anderer Länder zu respektieren.

Wir können lange darüber streiten, ob dies nicht bereits entsprechend den bestehenden internationalen rechtlichen Vereinbarungen verpflichtend ist. Wir können darüber streiten, ob die amerikanische Verfassung anwendbar ist oder nicht. Aber ich denke, die wichtigste Tatsache ist, dass die amerikanische Regierung begonnen hat, einen politischen Dialog zu führen, in dem die Verpflichtung demokratischer Regierungen zur Beachtung der Privatsphäre zumindest der Bürger anderer demokratischer Länder zur Sprache kommt. Und ich denke, hier gibt es, wenn die Bundesrepublik und die USA zusammen-

Original

democratic governments treat the citizens of each other's countries. And this is - I think it's important to emphasize - a reciprocal problem. As this committee, I understand, has begun to discover, there is not a single country that has clean hands on this subject. I'm not aware of any democratic country that has committed itself in its enacted laws to protect the privacy of citizens of other countries who are not in their own territory. And I think no country has, in my view, adequate laws to protect its own citizens, but none has any laws - and that's still the case in the United States - which provide protection for citizens of other countries.

But I think we now have the agreement in principle that that is something that democratic countries need to do. We have the European Court suggesting that, at least under European law, that is required. And, therefore, I think there is a real opportunity here, which I hope our two governments will seize, and that is to come together with other like-minded democratic governments to draft a set of principles, which each country would then agree to take back and enact into binding legislation, which would provide for adequate protection of the privacy of private citizens of all of our countries against surveillance.

Now, obviously, we need protection - as we've been learning again - from non-democratic governments who seem very interested in our private communications, and we need protection from just private citizens of all our countries who engage in illegal surveillance of our materials. But I think those are separate and different questions as is the question of whether governments should spy on other governments and, if so, in what ways and at what levels.

Deutsche Übersetzung

arbeiten, eine echte Gelegenheit, auf diesen ersten Schritt aufzubauen und eine Veränderung herbeizuführen, und zwar eine fundamentale Veränderung in der Art und Weise, wie demokratische Regierungen mit den Bürgern der jeweils anderen Länder umgehen. Und das ist - ich denke, dies ist wichtig zu betonen - ein gegenseitiges Problem. Wie dieser Ausschuss, soweit ich weiß, bereits herausgefunden hat, gibt es kein einziges Land, das in dieser Hinsicht eine weiße Weste hat. Mir ist kein demokratisches Land bekannt, das sich selbst gesetzlich verpflichtet hat, die Privatsphäre von Bürgern anderer Länder, die sich nicht auf dem Gebiet dieses Staates befinden, zu schützen. Meines Erachtens hat kein Land adäquate Gesetze zum Schutz der eigenen Bürger, und nicht ein einziges hat - und das gilt auch nach wie vor für die USA - ein einziges Gesetz verabschiedet, das die Bürger anderer Länder schützt.

Aber ich denke, jetzt haben wir im Prinzip die Übereinkunft, dass dies etwas ist, das demokratische Länder tun müssen. Wir haben den Europäischen Gerichtshof, der sagt, dass dies zumindest unter europäischem Recht verlangt wird. Und deswegen denke ich, es gibt hier eine echte Gelegenheit, von der ich hoffe, dass unsere Regierungen sie ergreifen, und zwar indem sie sich mit anderen gleichgesinnten demokratischen Regierungen zusammensetzen, um Grundsätze zu formulieren, die von den einzelnen Ländern dann in verbindliche nationale Gesetze gegossen werden, die den Bürgern unser aller Länder einen adäquaten Schutz ihrer Privatsphäre vor Überwachung bieten.

Nun müssen wir uns natürlich - wie wir gelernt haben - auch vor undemokratischen Regierungen schützen, die sich offenbar sehr für unsere private Kommunikation interessieren. Und wir müssen uns vor Privatpersonen in allen unseren Ländern schützen, die unser Datenmaterial illegal überwachen. Aber ich glaube, das sind voneinander getrennte und eigenständige Fragen, ebenso wie die Frage, ob Regierungen andere Regierungen ausspionieren sollten und, falls ja, auf welche Weise und in welchem Maße.

Original

Those are all important, hard questions, but they are separate from the one that I want to focus on, which is the surveillance by democratic governments of private citizens of other democratic countries who are not in their own territory. And I think we need to start with the principle that such surveillance should be subject to legal authority and should only take place subject to an enactment of laws which are legally binding and which have the public meaning that the average person would think they have. We need to move away from what the United States has done in the past and may still be doing now, which is to say that it has a private, secret interpretation of what the law means and says, "Don't worry, we're following the law", but that turns out to mean something very different.

So, what I would propose is that our two governments come together and agree that we are going to develop this protocol, agreement - whatever one would want to call it - which would then lead to the enactment of binding legislation, and that we would invite other like-minded democratic countries to join in this process, as I suggest in my paper. I think we also need to invite into those discussions civil society and businesses that are affected by this process. And this should be a multi-stakeholder discussion, which may obviously require some private conversations just among governments. But I think most of this could be discussed and should be discussed in a multi-stakeholder forum. And the notion would be to agree on a set of principles which would then be enacted into law.

The first principle, as I said, would be that these persons - I describe them as "protected persons" in my paper - could only be surveilled subject to legislation duly enacted into law and binding on the governments. Second, that the surveillance

Deutsche Übersetzung

Dies sind alles wichtige und schwierige Fragen, aber sie sind getrennt von der zu beantworten, auf die ich mich hier konzentrieren möchte. Mir geht es um die Überwachungsaktivitäten demokratischer Staaten gegen private Bürger anderer demokratischer Länder, die sich nicht auf dem Hoheitsgebiet dieser Staaten befinden. Und ich denke, wir brauchen zunächst den Grundsatz, dass eine solche Überwachung einer Rechtsgrundlage bedarf und verbindlichen Gesetzen unterliegen sollte, deren öffentlicher Wortlaut von Otto Normalverbraucher verstanden wird. Wir müssen von dem wegkommen, was die USA in der Vergangenheit getan haben und vielleicht immer noch tun, und zwar einer eigenen, geheimen Auslegung dessen, was in dem Gesetz steht und was es bedeutet, zu sagen: „Macht euch keine Sorgen, wir halten uns an das Gesetz"; allerdings sieht diese Auslegung dann ganz anders aus.

Ich schlage also vor, dass unsere beiden Regierungen zusammenkommen und vereinbaren, dass wir ein Protokoll, Abkommen - wie auch immer man es nennen will - entwickeln, das dann zur Verabschiedung verbindlicher Gesetze führt, und dass wir andere gleichgesinnte demokratische Länder auffordern, sich diesem Prozess anzuschließen, wie ich dies auch in meinem schriftlichen Statement vorgeschlagen habe. Ich denke, wir müssen in diese Diskussion auch den Bürger und jene Unternehmen, die von diesem Prozess betroffen sind, einbinden. Es sollte eine Diskussion mit vielen Akteuren sein, in der selbstverständlich auch einige nichtöffentliche Gespräche nur zwischen den Regierungen erforderlich sein werden. Doch ich glaube, das meiste könnte und sollte zwischen den zahlreichen Akteuren gemeinsam besprochen werden. Und der Gedanke dahinter wäre die Vereinbarung von Grundsätzen, die anschließend in nationale Gesetze umgesetzt würden.

Der erste Grundsatz wäre, wie bereits gesagt, dass diese Personen - ich nenne sie in meinem schriftlichen Statement „geschützte Personen" - nur unter geltenden, für die jeweiligen Staaten

Original

should be limited to specific purposes. There is a set of purposes that has been mentioned in the PPD; it's not narrow enough. But it is the fundamental principle that you move away from the notion that you can conduct surveillance just to gather foreign intelligence, where you don't have to suspect anybody of anything illegal. The American view has been that if two German private citizens are having a conversation, talking about what they think Germany might do, that's foreign intelligence information and can be collected. That is still the position of the American government and - I think - needs to change. There needs to be a set standard including criminal activity, and, obviously, there will be a debate about how to make that narrow enough so that you don't have a catch-all at the end that erases the communication.

We need, as has been suggested, to apply these rules to all forms of collection, not just bulk collection, which in the United States is a term of art, which means when you collect things with no sense at all of what you're collecting and who you're collecting it from. If you have any kind of indicators, for example, as far as I can tell, an indicator like "all cables from Afghanistan", then it's not bulk collection. And so, these rules have to apply to all forms of mass collection of data whether they're called bulk collection under the current law or not. And there need to be standards not only for the collection of this information, but for the retention of this information and for the sharing of this information, including sharing back to the government of the country that the person is a citizen of. And, obviously, there we need to make sure that governments don't collaborate with each other to get around restrictions in their own laws by simply having the other country collect the information.

Deutsche Übersetzung

verbindlichen Gesetzen überwacht werden dürfen. Zweitens sollte die Überwachung auf bestimmte Zwecke beschränkt sein. Die PPD nennt eine Reihe von Zwecken. Die sind aber nicht eng genug gefasst. Der eigentliche Grundsatz besteht jedoch darin, von der Idee wegzukommen, dass man Überwachungen durchführen kann, einfach um ausländische geheimdienstliche Informationen zu beschaffen, wenn es keinerlei Hinweise auf illegale Aktivitäten gibt. Der amerikanische Standpunkt ist der, dass, wenn zwei deutsche Privatpersonen sich darüber unterhalten, was Deutschland ihrer Meinung nach tun wird, dies ausländische geheimdienstliche Informationen sind und erfasst werden dürfen. Das ist nach wie vor die Ansicht der amerikanischen Regierung, und das muss sich - so denke ich - ändern. Es muss ein Standard festgelegt werden, der kriminelle Aktivitäten einschließt. Natürlich wird es eine Debatte darüber geben, wie sich dieser eng genug fassen lässt, sodass nicht ganz am Ende ein allumfassendes Kriterium dasteht, das die Absicht zunichtemacht.

Wie bereits vorgeschlagen wurde, müssen wir diese Regeln auf alle Arten der Erfassung anwenden, nicht nur die „Bulk Collection" [undifferenzierte massenhafte Erfassung], die in den USA ein Kunstbegriff ist, der bedeutet, dass man Dinge erfasst, ohne überhaupt eine Ahnung davon zu haben, was man erfasst und von wem es stammt. Insoweit aber irgendeine Art von Indikator vorgegeben ist, sagen wir, ein Indikator wie zum Beispiel „alle Telegramme aus Afghanistan", ist es dann keine Bulk Collection. Also müssen diese Regeln auf alle Arten der massenhaften Erfassung von Daten angewendet werden, und zwar unabhängig davon, ob sie nach geltendem Recht als „Bulk Collection" betitelt werden oder nicht. Und nicht nur für die Erfassung dieser Daten muss es Standards geben, sondern auch für deren Speicherung und Weitergabe, einschließlich der Weitergabe an die Regierung des Landes, dessen Bürger die betreffende Person ist. Und natürlich müssen wir dabei sicherstellen, dass Regierungen sich nicht zusammentun, um Beschränkungen in ihren eigenen Geset-

Original

Now there are obviously going to be difficulties in determining whether the person being surveilled is a protected person, the information being gathered is from a protected person. I think the starting point should be the assumption that if you collect information about a person, that is information from a protected person unless you have a reasonable basis to know that the person is not a protected person, because they're a citizen of a country that's outside the scope of the agreement or because they're a government official. And only then should you be able to proceed under different procedures.

There needs to be a commitment from each country to provide for effective oversight, and that will differ from country to country. Some countries have effective ombudsmen; the United States does not. But there needs to be effective administrative oversight, legislative oversight, and the possibility, as has already been suggested, of judicial oversight, so that the courts review the surveillance in advance, but also that there's a clear opportunity for people to challenge it and there is some procedure for challenging the legality of the surveillance and whether it's consistent with the agreed processes.

I think this process, if it went forward, would force all of our governments to think hard about what kinds of restrictions they want to put on and are willing to put on their own collection, with the added, for the first time, bonus that it would be protecting their own citizens from the surveillance of other countries, because they would be subject to the same limitations. This will not solve all of the problems, and it will only be useful and effective if at the same time we put more restrictions on our own citizens.

Deutsche Übersetzung

zen zu umgehen, indem sie die gewünschten Daten einfach von dem jeweils anderen Land erfassen lassen.

Nun wird es natürlich nicht immer leicht sein, festzustellen, ob die überwachte Person eine geschützte Person ist, die erfassten Daten von einer geschützten Person stammen. Ich denke der Ausgangspunkt sollte die Annahme sein, dass, wenn man Daten über eine Person sammelt, dies die Daten von einer geschützten Person sind, es sei denn, man verfügt über hinreichendes Wissen, dass die Person keine geschützte Person ist, etwa weil sie Bürger eines Landes ist, das nicht der Vereinbarung unterliegt, oder weil sie Staatsbediensteter ist. Und nur dann sollte eine andere Verfahrensweise zulässig sein.

Es muss eine Verpflichtung jedes Landes geben, eine effiziente Kontrolle zu schaffen, und die wird von Land zu Land unterschiedlich sein. Einige Länder haben effiziente Ombudsstellen. Die USA haben dies nicht. Doch es muss eine wirksame behördliche Kontrolle geben, ebenso wie eine Kontrolle vonseiten des Gesetzgebers und, wie bereits angeregt wurde, die Möglichkeit einer gerichtlichen Kontrolle, in deren Rahmen die Gerichte die Überwachung im Voraus prüfen können, es aber auch eine klare Möglichkeit für die Bürger gibt, sich gegen die Überwachung zur Wehr zu setzen, sowie ein Verfahren, in dem die Rechtmäßigkeit einer Überwachung und ihre Übereinstimmung mit der vereinbarten Vorgehensweise angefochten werden kann.

Ich denke, dieser Prozess würde, wenn es damit vorangeht, alle unsere Regierungen zwingen, sich genau zu überlegen, wie sie die Überwachung beschränken wollen und welche Beschränkungen sie ihren eigenen Erfassungsaktivitäten auferlegen wollen - und dies erstmals mit dem zusätzlichen Vorteil, dass es ihre eigenen Bürger gegen die Überwachung durch andere Länder schützt, weil diese denselben Beschränkungen unterliegen würden. Dies wird nicht alle Probleme lösen, und es wird nur nützlich und wirksam sein, wenn wir gleichzeitig zusätzliche

Original

Because even saying, as the Presidential Directive does, that the goal is to give the same privacy protection to foreigners abroad as we give to Americans at home, has to be caveated by the fact that we don't give much protection to the privacy of American citizens at home. So, we need to reform the standards for our own citizens as well as be willing to apply them to the citizens of other countries. But I think this process would force us to confront those issues and to deal with them in a way that would be more respectful of the privacy of our own citizens and the citizens of other countries.

Thank you very much.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank, Mr. Halperin. - Wir kommen jetzt zum nächsten Sachverständigen. Herr Soghoian, ich darf Ihnen das Wort für Ihr Eingangsstatement geben.

Sachverständiger Dr. Christopher Soghoian: I'd like to thank the committee of inquiry for giving me another opportunity to testify. As my colleague Ashley Gorski is also testifying at this hearing, I will leave it to her to speak on behalf of our employer, the ACLU. I'll be testifying today on my own behalf as a technologist and academic expert on government surveillance. As such, I wish to make it clear: the opinions I express are my own.

The disclosures by Edward Snowden changed the global conversation around surveillance. That is undeniable. Back in 2013, Snowden's disclosures landed like a political bombshell, providing the global public a chance to gawk at the American national security establishment's dirty laundry. At three years on, what impact did the disclosures have? If Edward Snowden's

Deutsche Übersetzung

Beschränkungen [zum Schutz] unserer eigenen Bürger einführen. Denn selbst wenn man sagt, wie es in der Direktive des Präsidenten steht, dass man die Privatsphäre von Ausländern im Ausland ebenso schützen will, wie man die Privatsphäre der Amerikaner in Amerika schützt, sollte man dabei nicht die Tatsache verschweigen, dass wir die Privatsphäre von amerikanischen Bürgern in Amerika nicht sonderlich gut schützen. Also müssen wir die Standards zugunsten unserer eigenen Bürger verbessern und zugleich bereit sein, sie auf die Bürger anderer Länder anzuwenden. Doch ich glaube, dieser Prozess würde uns dazu zwingen, uns diesen Problemen zu stellen und Lösungen zu finden, die einen respektvolleren Umgang mit der Privatsphäre unserer eigenen Bürger und der Bürger anderer Länder gewährleisten.

Ich danke Ihnen vielmals.

Sachverständiger Dr. Christopher Soghoian: *Vielen Dank dafür, dass ich erneut die Gelegenheit erhalten habe, vor dem Untersuchungsausschuss sprechen zu dürfen. Da meine Kollegin Ashley Gorski ebenfalls in dieser Anhörung aussagt, überlasse ich es ihr, im Namen unseres Arbeitgebers, der ACLU, zu sprechen. Ich werde heute in meinem eigenen Namen als Technologe und akademischer Gutachter für staatliche Überwachung aussagen. Insofern möchte ich klar zum Ausdruck bringen, dass die von mir geäußerten Meinungen meine eigenen sind.*

Die Enthüllungen von Edward Snowden haben die weltweite Debatte rund um das Thema Überwachung verändert. Das lässt sich nicht leugnen. Wie eine politische Bombe schlugen damals im Jahr 2013 Snowdens Enthüllungen ein und ließen die Weltöffentlichkeit einen ungläubigen Blick auf die schmutzige Wäsche des amerikanischen Sicherheitsdienstes NSA werfen. Welche

Original

impact is only measured by legal and legislative reforms and by the extent to which the NSA's activities are now effectively regulated by American courts and Congress, then, sadly, he probably should have stayed in Hawaii. James Clapper, the Director of National Intelligence, who lied to Congress and the American people about Section 215, metadata collection, kept his job. The American intelligence community continues to operate in near total secrecy. Our system of intelligence oversight remains a farce. And the most problematic intelligence activities that the NSA engages in - those that take place under Executive Order 12333 - are not overseen by the secretive FISA Court. Moreover, our two congressional intelligence committees, which are totally captured by the agencies they regulate, seem more focused on advocating for an expansion of the surveillance state's powers than reining them in.

This is not to say that Edward Snowden's brave act of whistleblowing did not have an impact. Snowden's disclosures had a massive impact, significantly improving the privacy and cyber security of every Internet-using person in the world. However, the most important changes have taken place in the technology community - not in the halls of Congress or in our secretive FISA Court. Snowden's disclosures were a much-needed wake-up call to the tech community and specifically the information security community. Snowden's disclosures radicalized a generation of engineers, students, researchers, and open-source advocates, the very people who design and build the software and hardware that NSA had, for years, quietly exploited.

Until just a few years ago, most data that flowed over the Internet and other global communications networks was unencrypted or encrypted

Deutsche Übersetzung

Folgen sind drei Jahre danach festzustellen? Würde man die Wirkung der Enthüllungen Snowdens ausschließlich an umgesetzten Rechts- und Gesetzesreformen messen und daran, inwieweit die Aktivitäten der NSA heute wirksam durch die amerikanischen Gerichte und den Kongress reguliert werden, dann müsste man wohl leider sagen, er hätte in Hawaii bleiben sollen. James Clapper, der Director of National Intelligence, der den Kongress und das amerikanische Volk in Bezug auf § 215, die Erfassung von Metadaten, anlog, hat seinen Job behalten. Die amerikanischen Geheimdienste arbeiten weiterhin nahezu vollkommen im Geheimen. Unsere Geheimdienstkontrolle ist nach wie vor eine Farce. Und die problematischsten Geheimdienstaktivitäten der NSA - jene, die unter EO 12333 stattfinden - werden vom geheimen FISA Court nicht kontrolliert. Zudem sind unsere beiden Kongressausschüsse zum Thema Geheimdienst von den Behörden, die sie regulieren sollen, vollkommen vereinnahmt und offensichtlich mehr darauf bedacht, sich für eine Erweiterung der staatlichen Überwachungsvollmachten einzusetzen, als darauf, diese einzugrenzen.

Ich will damit nicht sagen, dass Edward Snowdens mutiges Handeln als Whistleblower zu nichts geführt hat. Snowdens Enthüllungen hatten massive Auswirkungen, indem sie die Privatsphäre und Cybersicherheit jedes Internetnutzers auf der ganzen Welt deutlich verbessert haben. Doch die wichtigsten Änderungen haben in der Technologiebranche stattgefunden - nicht im Kongress oder in unserem geheimen FISA Court. Snowdens Enthüllungen waren ein dringend notwendiger Weckruf für die Technologiebranche und insbesondere die Datensicherheitsbranche. Snowdens Enthüllungen haben eine ganze Generation von Ingenieuren, Studenten, Forschern und Open-Source-Befürwortern radikalisiert, eben die Menschen, die die Software und Hardware entwickeln, die von der NSA jahrelang still und leise ausgenutzt wurde.

Bis vor wenigen Jahren waren die meisten Daten, die über das Internet und andere globale Netzwerke flossen, unverschlüsselt oder nur mit

Original

with weak encryption algorithms that offered no real protection. This meant that most emails, text messages, phone calls, search queries, and social media content could be intercepted by the NSA and other well-resourced intelligence agencies. For the NSA and its Five Eyes partners, the big challenge was in acquiring the communications data and then making sense of it. That meant quietly partnering with global communications companies who operate international fiber-optic cables and investing in data-mining technology so that analysts could sift through the massive amounts of data that had been collected.

The real scandal wasn't that the NSA and its partners were spying on the world's communications, but that these communications were so poorly secured that they could be collected in bulk in the first place. Why was so much private data either unencrypted or poorly encrypted? Now, the so-called "Crypto Wars" are certainly responsible for some of this. For years, Western governments sought to prevent the mass deployment of cryptography through legislation and lobbying technical standards organizations. The impact of these policies is perhaps the greatest in the telecommunications industry, and it is unlikely that this will change any time soon. Landline and cellular phone calls using services offered by incumbent carriers are unencrypted today and will likely still be unencrypted in five years and in ten years. The reasons for this are complicated, but the long, deep relationships between telecommunications carriers and intelligence services probably aren't helping things.

Deutsche Übersetzung

schwachen Verschlüsselungsalgorithmen, die keinen wirklichen Schutz boten, verschlüsselt. Das heißt, dass die meisten E-Mails, Textnachrichten, Telefongespräche, Suchanfragen und Social-Media-Inhalte von der NSA und anderen Geheimdiensten, die über entsprechende Mittel verfügten, abgefangen werden konnten. Für die NSA und ihre Five-Eyes-Partner lag die große Schwierigkeit darin, die Kommunikationsdaten zu beschaffen und dann herauszufinden, was sie bedeuteten. Dazu mussten sie im Stillen mit weltweiten Kommunikationsunternehmen, die internationale Glasfaserkabel betreiben, zusammenarbeiten und in Data-Mining-Technologien investieren, sodass Analysten die enormen Mengen erfasster Daten entsprechend filtern konnten.

Der eigentliche Skandal bestand nicht darin, dass die NSA und ihre Partner die weltweite Kommunikation ausspionierten, sondern dass diese Kommunikation so schlecht gesichert war, dass sie überhaupt erst massenweise erfasst werden konnte. Warum war so viel private Kommunikation entweder unverschlüsselt oder schlecht verschlüsselt? Nun, zum Teil lässt sich das sicherlich auf die sogenannten „Crypto Wars" [Verschlüsselungskriege] zurückführen. Jahrelang haben die westlichen Regierungen sich bemüht, den massenhaften Einsatz von Kryptographie durch Gesetzgebung und Lobbyismus bei den technischen Normungsorganisationen zu verhindern. Die Telekommunikationsbranche ist möglicherweise am meisten von dieser Politik beeinflusst, und es ist unwahrscheinlich, dass sich dies in nächster Zeit ändern wird. Noch heute sind Festnetz- und Mobiltelefongespräche über die Dienste der vorherrschenden Telekommunikationsunternehmen unverschlüsselt, und es ist anzunehmen, dass sie auch noch in fünf und in zehn Jahren unverschlüsselt sein werden. Die Gründe hierfür sind kompliziert, aber die langjährigen und intensiven Beziehungen zwischen Telekommunikationsunternehmen und Geheimdiensten machen es wahrscheinlich nicht leichter.

Nur zur dienstlichen Verwendung

Original

The Crypto Wars and pressure by Western governments cannot, however, be blamed for the failure of the technology industry to embrace strong encryption. The fact is that until recently the tech community just did not take security seriously. Even before the Snowden disclosures, some tech companies were starting to embrace strong encryption technology. Google enabled HTTPS by default in January of 2010, which protected the communications of Google users as they were using open communications networks. In the years that followed, Twitter and Facebook also adopted HTTPS in 2012 and 2013 respectively. These companies have not just led the industry on the use of default encryption for the Web, but they have also pushed the industry forward in other areas, promoting the use of stronger encryption algorithms, encryption between email servers, and certificate transparency. The emerging tech industry's best practice of a strong encryption, enabled by default, which had begun before Snowden, snowballed after his disclosures. Companies like Yahoo, which had long resisted public pressure to use HTTPS, were finally shamed into compliance once *The Washington Post* revealed that the NSA was collecting data from twice as many Yahoo users as any other webmail service.

Three years after Snowden blew the whistle, the encryption landscape looks very different. WhatsApp has delivered end-to-end encryption, enabled by default, to a billion users. Apple has enabled strong default encryption of data stored on mobile devices. And the use of default HTTPS has spread from technology companies to even the U.S. government, which is now requiring that it be enabled by all government agencies by the end of 2016, and even to the media: major U.S. news organizations like *The Washington Post*, BuzzFeed and *Politico* have all enabled it by default.

Deutsche Übersetzung

Die Crypto Wars und der von den westlichen Regierungen ausgeübte Druck können jedoch nicht allein als Grund für das fehlende Interesse der Technologiewirtschaft an starker Verschlüsselung herhalten. Vielmehr hat die Technologiebranche das Thema Sicherheit bis vor kurzem einfach nicht ernst genommen. Schon vor den Snowden-Enthüllungen fingen einige Technologieunternehmen an, starke Verschlüsselungstechnologien einzuführen. Im Januar 2010 machte Google HTTPS zum Standard und schützte so jede über offene Netzwerke stattfindende Kommunikation von Google-Usern. Daraufhin führten auch Twitter und Facebook in den Jahren 2012 bzw. 2013 HTTPS ein. Diese Unternehmen waren nicht nur die Vorreiter der Branche in der standardmäßigen Verschlüsselung im Internet, sondern haben sie auch dazu gedrängt, in anderen Bereichen stärkere Verschlüsselungsalgorithmen, Verschlüsselung zwischen E-Mail-Servern und Zertifikatstransparenz voranzutreiben. Das in der Technologiewirtschaft aufkommende bestmögliche Verfahren zur standardmäßigen starken Verschlüsselung, die schon vor Snowden begonnen hatte, nahm nach den Enthüllungen exponentiell zu. Unternehmen wie Yahoo, die dem öffentlichen Druck, HTTPS zu verwenden, lange standgehalten hatten, knickten letztlich ein und erfüllten die Forderung, als die „Washington Post" herausfand, dass die NSA doppelt so viele Daten von Yahoo-Usern erfasste wie von anderen Webmailern.

Drei Jahre nachdem Snowden Alarm schlug, sieht die Verschlüsselungslandschaft anders aus. WhatsApp bietet einer Milliarde Usern die standardmäßige End-to-End-Verschlüsselung. Apple hat eine standardmäßige starke Verschlüsselung aller auf mobilen Geräten gespeicherten Daten eingeführt. Und die Verwendung von standardmäßigem HTTPS hat sich nicht nur unter den Technologieunternehmen durchgesetzt, sondern auch bei der US-Regierung, die jetzt verlangt, dass der Standard bis Ende 2016 in allen Regierungsbehörden eingeführt wird. Und selbst bei den Medien: Die großen US-Medienunternehmen wie die „Washington Post",

Nur zur dienstlichen Verwendung

Original

The tech industry's embrace of encryption has almost certainly had a significant impact on the activities of intelligence agencies. Bulk surveillance of many previously unencrypted communications is no longer possible, forcing governments to either demand data from technology companies or to directly hack end users. To be clear: this change isn't entirely due to Snowden. But his disclosures certainly helped. Where Snowden had the greatest impact, however, is in the attitudes of the engineers who design the technologies that we all use.

The technology community has a bad track record when it comes to designing secure protocols and technical standards. Far too many technologies have emerged from standards committees that include weak, insecure options, often enabled by default. Rather than embracing protocols and algorithms that are secure by default, technical standards bodies have for far too long produced bloated, insecure protocols, often with encryption algorithms known to be weak. In part, this was because security concerns were not taken seriously, and partly out of a desire to make everyone involved in the standards process happy. This is starting to change - in large part due to the Snowden disclosures.

There is a political science concept called an "Overton window", which is the range of ideas considered politically acceptable in the current climate of public opinion. Prior to Snowden's disclosures, many engineers, including those involved in technical standards bodies, simply did not take security concerns seriously, particularly if they involved the activities by NSA or other intelligence services. Those who raised such

Deutsche Übersetzung

BuzzFeed und „Politico" haben es alle als Standard eingeführt.

Die Hinwendung der Technologiebranche zur Verschlüsselung hat die Arbeit der Geheimdienste mit hoher Sicherheit deutlich erschwert. Die massenhafte Überwachung vieler zuvor unverschlüsselter Kommunikationen ist nicht mehr möglich, sodass die Regierungen die Daten entweder von den Technologiefirmen verlangen oder die Systeme der Endnutzer direkt hacken müssen. Um es klar zu sagen: Dieser Wandel ist nicht allein auf Snowden zurückzuführen. Aber seine Enthüllungen haben sicherlich ihren Teil dazu beigetragen. Vor allem hat Snowden jedoch die Einstellung der Entwickler verändert, von denen die Technologien, die wir alle nutzen, stammen.

Die Technologiebranche hat in der Vergangenheit bei der Entwicklung sicherer Protokolle und technischer Standards keine gute Arbeit geleistet. Viel zu viele der aus den Normenausschüssen hervorgegangenen Technologien bieten schwache, unsichere Optionen, die nicht selten als Standard aktiviert werden. Anstatt Protokolle und Algorithmen zu favorisieren, die von sich aus sicher sind, haben die für Normung verantwortlichen Stellen viel zu lange aufgeblähte, unsichere Protokolle geliefert, von deren Verschlüsselungsalgorithmen man oft wusste, dass sie unsicher waren. Zum Teil lag dies daran, dass Sicherheitsfragen nicht ernst genommen wurden, und zum Teil an dem Wunsch, mit allen an dem Normungsprozess beteiligten Parteien auf einen Nenner zu kommen. Hier beginnt man, umzudenken, und zwar zu einem großen Teil aufgrund der Snowden-Enthüllungen.

In der Politikwissenschaft gibt es den Begriff des „Overton-Fensters", das die Bandbreite der Ideen bezeichnet, die im jeweils aktuellen öffentlichen Meinungsklima politisch annehmbar sind. Vor Snowdens Enthüllungen nahmen viele Entwickler, einschließlich derer, die in den technischen Normungsgremien saßen, Sicherheitsfragen schlicht nicht ernst, insbesondere wenn

Original

concerns were easily dismissed as being paranoid. The Overton window simply did not consider nation-state actors.

Today, security concerns are far more likely to be taken seriously, and the potential exploitation of weak security technologies by nation-state actors is far tougher to dismiss as unreasonable paranoia. Moreover, an entire generation of researchers have been inspired to create new technologies that specifically seek to protect users from nation-state adversaries. To be clear: this does not mean that all of the protocols, standards and technologies in use are now secure; they're not. There are many, many old insecure technologies that are still in use, and it will take a long time and a lot of money to get rid of them. Inertia is very hard to overcome. But hopefully, going forward, many of the new communications technologies will be much harder for nation states to exploit and surveil in bulk.

Intelligence reforms and oversight have their place, but they are no substitute for good cyber security. The American government may promise to restrict the NSA's activities, either by not spying on your Chancellor or increasing the privacy protections afforded to your citizens. Certainly such assurances would be nice, but it would not be wise to rely on them.

First, intelligence agencies operate in the shadows. And when they inevitably chafe at the laws that restrict them, they either find loopholes or simply break the law. There is a long history of intelligence agencies breaking surveillance laws they find inconvenient in the United States, in the U.K., and even here in Germany.

Deutsche Übersetzung

sie die Aktivitäten der NSA oder anderer Geheimdienste betrafen. Wer solche Fragen aufwarf, wurde schnell als paranoid abgestempelt. Staatliche Akteure lagen einfach außerhalb des Overton-Fensters.

Heute ist es weitaus wahrscheinlicher, dass Sicherheitsfragen ernst genommen werden. Und die potenzielle Ausnutzung schwacher Sicherheitstechnologien durch staatliche Akteure als unangebrachte Paranoia abzutun, ist viel schwieriger. Außerdem ist eine ganze Generation von Wissenschaftlern dazu motiviert worden, neue Technologien speziell zum Schutz von Usern gegen staatliche Angreifer zu entwickeln. Um dies klarzustellen: Das bedeutet nicht, dass jetzt alle aktuell verwendeten Protokolle, Standards und Technologien sicher sind. Das sind sie nicht. Es gibt viele, viele alte und unsichere Technologien, die immer noch in Gebrauch sind. Und es wird viel Zeit und Geld kosten, sie loszuwerden. Trägheit ist sehr schwer zu überwinden. Aber hoffentlich werden es viele der neuen Kommunikationstechnologien den Staaten zukünftig schwerer machen, sie auszunutzen und eine massenhafte Überwachung durchzuführen.

Geheimdienstreformen und -kontrolle sind gut, aber eine gute Cybersicherheit können sie nicht ersetzen. Die amerikanische Regierung mag vielleicht versprechen, die Aktivitäten der NSA zu begrenzen, indem sie aufhört, Ihre Kanzlerin auszuspionieren, oder den Schutz der Privatsphäre Ihrer Bürger erhöht. Sicher wären solche Zusicherungen wünschenswert, aber es wäre nicht weise, sich darauf zu verlassen.

Erstens operieren Geheimdienste im Schatten. Und wenn sie sich über die Gesetze ärgern, die ihnen Beschränkungen auferlegen, was unvermeidbar ist, dann finden sie entweder Lücken darin oder setzen sich einfach darüber hinweg. Viele Male haben Geheimdienste in den USA, dem Vereinigten Königreich und sogar hier in Deutschland in der Vergangenheit Gesetze gegen Überwachung gebrochen, die ihnen im Weg waren.

Original

Second, the NSA is not the only intelligence agency that is spying on the communications of Germans. The foreign intelligence services of Russia, China, the United Kingdom, France and Israel will simply not be bound by restrictions that the U.S. government imposes on the NSA.

The only effective way to protect your government's communications and the data of German companies and citizens is to embrace strong cyber security technologies. This will take political will, the investment of significant sums of money, bold action by data security regulators, and a willingness by politicians to prioritize cyber security over domestic law enforcement concerns.

Thank you again for the invitation to testify today. I appreciate the committee's interest in the topic and would be happy to answer any questions you have.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank für Ihr Eingangsstatement, Herr Soghoian. - Wir kommen jetzt, last, but not least, zu Amie Stepanovich, zu ihrem Eingangsstatement. Wir freuen uns darauf.

Sachverständige Amie Stepanovich: Thank you very much. - Dr. Soghoain is always a hard act to follow, but I want to start by thanking the members of the committee on behalf of Access Now and on behalf of myself for inviting me to Berlin, for holding this hearing, and for considering this incredibly important matter. My full written testimony is available on the record, but here I want to take this opportunity to emphasize three points that I think are incredibly significant to your considerations.

The first is that the reforms we've seen since 2013 are not adequate to address the question of U.S. surveillance of Germans and others around

Deutsche Übersetzung

Zweitens ist die NSA nicht der einzige Geheimdienst, der die Kommunikation von Deutschen ausspioniert. Die Geheimdienste von Russland, China, dem Vereinigten Königreich, Frankreich und Israel werden schlicht und einfach nicht an Beschränkungen gebunden sein, die die US-Regierung der NSA auferlegt.

Der einzig wirksame Weg, die Kommunikation Ihrer Regierung und die Daten deutscher Unternehmen und Bürger zu schützen, ist die Einführung starker Cybersicherheitstechnologien. Dazu braucht es politischen Willen, erhebliche Investitionen, ein beherztes Handeln der Datenschutzbehörden und die Bereitschaft der Politik, Cybersicherheit über die Belange der nationalen Strafverfolgung zu stellen.

Vielen Dank dafür, dass ich heute hier aussagen durfte. Ich bedanke mich für das Interesse des Ausschusses an dem Thema und antworte gern auf etwaige Fragen Ihrerseits.

Sachverständige Amie Stepanovich: *Vielen herzlichen Dank. - Mit meinem Vorredner Dr. Soghoian mitzuhalten, ist immer schwer; aber zunächst möchte ich den Ausschussmitgliedern im Namen von Access Now und in meinem eigenen Namen dafür danken, dass sie mich nach Berlin eingeladen haben, dafür dass sie diese Anhörung durchführen, und dafür, dass sie sich mit diesem unglaublich wichtigen Thema befassen. Meine vollständige schriftliche Stellungnahme liegt Ihnen vor. Hier möchte ich jedoch die Gelegenheit nutzen, drei Punkte zu betonen, die ich als unheimlich wichtig für Ihre Erwägungen erachte.*

Der erste ist, dass die seit 2013 umgesetzten Reformen hinsichtlich der Überwachung deutscher und anderer Bürger weltweit durch die USA keine adäquaten Lösungen liefern. Wie meine

Original

the world. There have been, as my esteemed colleagues before me have indicated, two primary reform vehicles since the first Snowden revelations in 2013: the USA Freedom Act and Presidential Policy Directive 28.

The USA Freedom Act is the first time NSA surveillance has actually been statutorily limited in decades. And, in that, we think that it is incredibly significant to draw attention to its provisions: not only to limit NSA surveillance but also to increase both the transparency of surveillance from the U.S. government as well as from the companies that provide information. The USA Freedom Act was necessary because the U.S. government had requested - and the secret Foreign Intelligence Surveillance Court had approved - a secret reinterpretation of U.S. law that allowed them to collect massive amounts of information that previously we did not think possible under that authority. Whilst the USA Freedom Act applies both to U.S. persons and non-U.S. persons equally, because it really only applies to surveillance collected in the United States, it will only have a primary impact there.

Now, the second reform vehicle that I want to talk about really is necessary, because while the U.S. government ratified the International Covenant on Civil and Political Rights in 1992, it asserts that the obligations assumed by a state party to the ICCPR apply only within the territory of the state party. This means that there is no necessity or proportionality determination made when conducting extraterritorial surveillance in the United States. What the United States has not done in the Presidential Policy Directive, is extend the recognition of human rights to non-U.S. persons. Instead, what they have said is that all persons have legitimate privacy interests in the handling of their information. And this falls incredibly short of their ICCPR obligations to Germans and to foreign citizens. The Presidential Policy Directive, we

Deutsche Übersetzung

verehrten Kollegen bereits erwähnt haben, sind seit den ersten Snowden-Enthüllungen im Jahr 2013 zwei primäre Reforminstrumente verabschiedet worden: der USA Freedom Act und die Presidential Policy Directive 28.

Mit dem USA Freedom Act wird die Überwachung durch die NSA praktisch das erste Mal seit Jahrzehnten gesetzlich beschränkt. Und insofern halten wir es für äußerst wichtig, auf die darin enthaltenen Bestimmungen aufmerksam zu machen. Sie bedeuten nicht nur eine Beschränkung der Überwachungsaktivitäten der NSA, sondern auch erhöhte Transparenz hinsichtlich der von der US-Regierung durchgeführten Überwachungen und der Unternehmen, die Daten bereitstellen. Der USA Freedom Act war notwendig, weil die US-Regierung eine geheime Neuauslegung des US-Rechts, das ihr eine massenhafte Datenerfassung erlaubt, die wir unter diesen Vollmachten nicht für möglich gehalten hätten, gefordert und vom Foreign Intelligence Surveillance Court genehmigt bekommen hat. Auch wenn der USA Freedom Act sowohl auf Nicht-US-Personen wie auf US-Personen anwendbar ist, wird er, weil er wirklich nur für Überwachungsdaten Anwendung findet, die in den USA erfasst werden, nur dort unmittelbare Auswirkungen haben.

Das zweite Reforminstrument, über das ich sprechen möchte, ist wirklich notwendig; denn obwohl die US-Regierung im Jahr 1992 den Internationalen Pakt über bürgerliche und politische Rechte [ICCPR] ratifiziert hat, behauptet sie, dass die mit dem ICCPR übernommenen Verpflichtungen eines Staates nur auf dem Gebiet dieses Staates gelten. Das bedeutet, dass keine Notwendigkeit vorliegen muss oder Abwägung der Verhältnismäßigkeit stattfindet, wenn die USA von ihrem Gebiet aus Auslandsüberwachung betreiben. Mit der Presidential Policy Directive haben die USA nicht etwa ihre Anerkennung der Menschenrechte auf Nicht-US-Personen ausgeweitet. Was sie stattdessen damit sagen, ist, dass alle Menschen ein legitimes Recht auf Privatsphäre im Umgang mit ihren Daten haben. Und damit bleiben sie weit hinter

Original

would say, is mostly symbolic. And whilst it is an incredibly important symbol, it does not do enough and it contains several loopholes and qualifications that limit its application. And at the end of the day, it's right in the title: this is a policy directive. It is a policy statement. And since it is not imbued in law or even executive order, it is not necessarily going to apply to any future administration elected to take the presidency of the United States.

Which leads me to my second point: that the U.S. has shown little appetite to curb its extraterritorial surveillance or to recognize the human rights of people outside the country. In fact, recently there have been steps taken to increase their authority to collect information, which arguably outweigh the steps taken to limit surveillance, at least for non-U.S. persons outside the United States.

Notably, the Foreign Intelligence Surveillance Act Amendments Act, or FAA, which includes Section 702, which, as my colleague Ashley Gorski has explained, contains both authority for Prism and Upstream, will sunset late next year. Which means we're in the same situation we were with Section 215, where it sunsetted[1] last year and where we were able to get the political will to pass the USA Freedom Act to limit that authority. However, Congress has not even begun really to discuss what the reform of Section 702 and the other FAA provisions will look like. And what it seems that we are most likely to get out of that sunset is a limitation on the search of 702 databases for U.S. person information without a warrant, and not necessarily to the limits

Deutsche Übersetzung

ihren Verpflichtungen nach dem ICCPR gegenüber den Deutschen und Bürgern anderer Länder zurück. Wir würden sagen, die Presidential Policy Directive ist größtenteils symbolisch. Und obwohl sie ein äußerst wichtiges Symbol ist, reicht sie nicht aus, und sie enthält verschiedene Lücken und Bedingungen, die ihre Anwendung beschränken. Im Grunde steht es sogar schon im Titel: Dies ist eine politische Direktive. Es ist eine politische Erklärung. Und da sie nicht im Gesetz verankert oder wenigstens eine Rechtsverordnung ist, wird sie für eine zukünftige gewählte Regierung der USA nicht zwangsläufig verbindlich sein.

Womit ich auf meinen zweiten Punkt zu sprechen komme: Die USA haben wenig Lust gezeigt, ihre gebietsfremde Überwachung einzudämmen oder die Menschenrechte der Bürger anderer Länder anzuerkennen. Kürzlich wurden sogar Schritte unternommen, ihre Vollmachten zur Datenerfassung auszuweiten, welche die Schritte, die zur Eindämmung der Überwachung unternommen wurden, zumindest in Bezug auf Nicht-US-Personen außerhalb der USA möglicherweise aufheben.

Zu beachten ist, dass der Foreign Intelligence Surveillance Act Amendments Act [FAA, Änderungsgesetz zum Gesetz über Überwachungsmaßnahmen in der Auslandsaufklärung], der der § 702 enthält, der, wie meine Kollegin Ashley Gorski erklärt hat, die Rechtsgrundlage sowohl für Prism als auch für Upstream darstellt, im nächsten Jahr ausläuft. Wir sind also in derselben Situation wie mit § 215, als dieser im letzten Jahr auslief und wir den politischen Willen aufbringen konnten, zur Einschränkung dieser Rechtsgrundlage den USA Freedom Act zu verabschieden. Doch der Kongress hat noch nicht einmal begonnen, wirklich darüber zu sprechen, wie die Reform von § 702 und der

[1] Richtigstellung des SV: streichen von ‚where it sunsettet', setzen von: ‚part oft he USAPATRIOT Act that had a sunset date…', setzen von: ‚Because of the sunset'… , streichen von: ‚and where', setzen von: ‚we were able to get the political will to pass the USA Freedom Act to …', streichen von: ‚limit reform', siehe Anlage 1

Original

of data collected of non-U.S. persons. And then, in the law enforcement context, surveillance authorities are potentially increasing.

I'd like to draw your attention to a draft law that was recently published to amend the Electronic Communications Privacy Act in order to allow bilateral agreements between countries with the goal of providing direct, reciprocal access[2] to order the production of user information from companies located in other jurisdictions. The draft law would be precedent-setting in the United States, in that it will actually write human rights into U.S. statute, but the standard for the human rights is too weak. So, to understand why, I want to indicate that the first country that the U.S. is likely to enter into an agreement with under this draft law is the United Kingdom, the home to GCHQ. The UK already has arguably much broader surveillance authorities with much less oversight than the U.S. National Security Agency. And once passed - and it's being taken back up again tomorrow in the UK House of Lords - the Investigatory Powers Bill will give even broader authority with only the illusion of oversight. Whilst the agreement between the U.S. and the UK would ensure some protections for their own citizenry, they would not include any protections for citizens located elsewhere in the world, including Germany. This will not change the substance of surveillance authority, but it will give a much broader application to undermine the privacy of users around the world by allowing the UK to get direct access to information of Germans held by U.S. companies without going through mutual legal assistance treaties, as is now the case.

Deutsche Übersetzung

übrigen Bestimmungen des FAA aussehen sollen. Was uns das Auslaufen des Gesetzes wahrscheinlich bringen wird, ist eine Beschränkung der Durchsuchung ohne richterlichen Beschluss von Datenbanken gemäß § 702 nach Daten von US-Personen und nicht notwendigerweise eine Begrenzung der Erfassung von Daten von Nicht-US-Personen. Zudem werden Überwachungsvollmachten im Zusammenhang mit Strafverfolgung potenziell ausgeweitet.

Ich würde Sie gern auf einen kürzlich veröffentlichten Gesetzesentwurf aufmerksam machen, der den Electronic Communications Privacy Act [Gesetz über Privatsphäre in der elektronischen Kommunikation] abändern soll, um bilaterale Vereinbarungen zwischen Ländern dahin gehend zu ermöglichen, dass man über das jeweils andere Land direkt und gegenseitig von Unternehmen in anderen Rechtsordnungen die Herausgabe von Nutzerdaten verlangen kann. Der Gesetzentwurf wäre in den USA insofern richtungsweisend, als er tatsächlich Menschenrechte in US-Gesetze niederschreibt; jedoch ist der Standard für die Menschenrechte zu schwach. Um also zu erklären, warum das so ist, möchte ich darauf hinweisen, dass das erste Land, mit dem die USA wahrscheinlich eine Vereinbarung unter diesem Gesetz abschließt, das Vereinigte Königreich ist, die Heimat des GCHQ. Das Vereinigte Königreich hat wohl weit größere Vollmachten zur Überwachung und wird weitaus weniger kontrolliert als die U.S. National Security Agency. Und sobald es verabschiedet ist - morgen wird es wieder dem House of Lords vorgelegt -, wird das britische Überwachungsgesetz, die Investigatory Powers Bill, noch mehr Vollmachten bringen, mit einer bloßen Illusion der Kontrolle. Die Vereinbarung zwischen den USA und dem Vereinigten Königreich würde zwar ihren jeweiligen Bürgern einen gewissen Schutz bieten, für Bürger aller anderen Länder der Welt, einschließlich Deutschland, würde sie jedoch keinen Schutz bedeuten. Dies

[2] Ergänzung der SV: ‚for other governments', streichen von: 'other jurisdictions', hinzufügen von: 'the United States'

Original

Several of my colleagues have also brought up the Schrems case. And one important limitation - - My colleague Mr. Edgar talked about how the Schrems case will allow another opportunity for Europeans to press for reform. But I actually think that that opportunity has been severely limited by the U.S. Congress. This is because they actually took a very last-minute step in the passage of the Judicial Redress Act, or the JRA. Many of you might be familiar with the JRA. It was a necessary precondition to the adoption of the umbrella agreement between the EU and the United States. And it was supposed to extend certain U.S. Privacy Act protections to EU citizens, so that they could have some guarantee of protection and redress against U.S. government collection of their data. We, Access Now, had indicated that the JRA was going to be a small step forward for the rights of Europeans within the Unites States. However, at the very last minute, the U.S. Senate actually gutted that protection, and what would have been half a step forward became a huge step back. What happened was that the Senate included a provision that said that no country could qualify for the Privacy Act protections which had impeded the national security interests of the United States. This means that if the EU starts to place pressure on the United States to limit its surveillance of EU citizens, EU countries could find themselves stripped of their ability to get JRA status, which means that even the limited redress that has been provided could be taken away. This not only means that in the Privacy Shield negotiations EU interests were severely hampered, but in the future they will continue to be hampered and they will continue to be limited in how

Deutsche Übersetzung

wird die Rechtsgrundlagen der Überwachung inhaltlich nicht ändern; aber es wird die Untergrabung der Privatsphäre von Usern rund um die Welt befördern, indem es dem Vereinigten Königreich erlaubt, direkt auf Daten von Deutschen, die von US-Unternehmen gehalten werden, zuzugreifen, ohne über gegenseitige Rechtshilfeabkommen gehen zu müssen, wie es jetzt noch der Fall ist.

Mehrere meiner Kollegen haben auch den Schrems-Fall angesprochen. Und eine wichtige Beschränkung - - Mein Kollege Herr Edgar hat erklärt, wie der Schrems-Fall den Europäern eine weitere Möglichkeit gibt, auf Reformen zu drängen. Doch ich denke, dass der US-Kongress dieser Möglichkeit im Grunde bereits enge Grenzen gesetzt hat. Sie haben nämlich in letzter Minute vor Verabschiedung des Judicial Redress Act [JRA; in etwa: Gesetz für gerichtliche Wiedergutmachung] einen Schritt zurück gemacht. Viele von Ihnen werden mit dem JRA vertraut sein. Es war eine notwendige Voraussetzung für die Annahme des Umbrella Agreement zwischen der EU und den USA. Es sollte bestimmte Schutzbestimmungen des U.S. Privacy Act zugunsten von EU-Bürgern ausweiten und diesen einen gewissen Schutz sowie ein Beschwerderecht im Falle der Erfassung ihrer Daten durch die US-Regierung garantieren. Wir von Access Now hatten darauf hingewiesen, dass der JRA ein kleiner Schritt in die richtige Richtung für die Rechte von Europäern in den USA wäre. In letzter Minute kippte der US-Senat diesen Schutz jedoch. Und was ein halber Schritt nach vorn gewesen wäre, wurde zu einem großen Schritt zurück. Der Senat nahm eine Bestimmung auf, die besagt, dass kein Land den Schutz des Privacy Act in Anspruch nehmen kann, das zuvor die nationalen Sicherheitsinteressen der USA behindert hat. Das bedeutet, dass, wenn die EU anfängt, die USA zu drängen, ihre Überwachung von EU-Bürgern einzuschränken, den EU-Ländern hierfür ihre Ansprüche unter dem JRA entzogen werden können, was bedeutet, dass selbst die begrenzten Beschwerderechte, die gewährt wurden, zurückgenommen werden könnten. Das bedeutet nicht nur, dass in den Privacy-

Original

much they can exert pressure on U.S. surveillance.

Finally, I want to spend some time on the steps that the U.S. is taking to ensure its ability to maintain access to data - what is often called "exceptional access" - as opposed to its authority to do so. As my colleague Dr. Soghoian has testified: perhaps one of the best outcomes of the Snowden revelations is the increased use of secure communications technologies. This is something that has been a long time coming and is increasingly important to 21st century interactions. It protects against bad actors gaining access to information as well as data breaches. And I think we can all agree that the last thing that the world needs is an increase in the number of data breaches that we hear about in the news every day. Encryption lies at the heart of this. And right now, thankfully, no U.S. law on its face inhibits the ability of U.S. companies or U.S. persons to develop or use strong encryption; in fact, several policies promote its use, and with good reason.

However, the Federal Bureau of Investigation has been on a multi-decade war to limit encryption, starting in the 1990s. But today they are seeking to prevent the use of what is called "end-to-end encryption", the type of encryption deployed by WhatsApp, Signal and Apple's iMessage in order to make sure that only the intended sender and the receiver of information can get access to those communications. And it's not only the FBI that is seeking to limit encryption. India, China, the UK - whom China actually praised when passing its own law limiting end-to-end encryption - as well as, unfortunately, both France and Germany have been seeking to limit encryption - both development and use.

Deutsche Übersetzung

Shield-Verhandlungen die Interessen der EU beschnitten worden sind, sondern dass sie auch in Zukunft weiterhin beschnitten werden und dass der Druck, den man auf die US-Überwachung ausüben können wird, weiterhin begrenzt bleibt.

Zum Schluss möchte ich noch ein bisschen Zeit darauf verwenden, die Schritte zu beleuchten, die die USA unternehmen, um sich den Zugriff auf Daten zu sichern - was oft als „ausnahmsweiser Zugriff" bezeichnet wird - im Gegensatz zu ihren Vollmachten, dies zu tun. Wie mein Kollege Dr. Soghoian ausgesagt hat, ist eine der vielleicht positivsten Auswirkungen der Snowden-Enthüllungen der zunehmende Einsatz sicherer Kommunikationstechnologien. Das ist etwas, was sich langsam entwickelt hat und immer wichtiger wird für unsere Interaktionen im 21. Jahrhundert. Diese Technologien schützen vor missbräuchlichem Zugriff auf Daten sowie vor Verstößen gegen datenschutzrechtliche Bestimmungen. Und ich denke, wir sind uns alle einig, dass die Welt nichts weniger braucht als eine Zunahme der Verstöße gegen den Datenschutz, von denen wir dann täglich in den Nachrichten hören. Die Lösung heißt Verschlüsselung. Und zum jetzigen Zeitpunkt hindert, glücklicherweise, scheinbar kein US-Gesetz Unternehmen oder Bürger der USA an der Entwicklung oder Nutzung starker Verschlüsselung. Verschiedene politische Initiativen fördern sogar ihre Verwendung, und zwar aus gutem Grund.

Bereits in den 1990er-Jahren hat jedoch das Federal Bureau of Investigation [FBI] der Verschlüsselung den Krieg angesagt und versucht, sie seither zu begrenzen. Heute gilt sein Kampf allerdings dem Einsatz der End-to-End-Verschlüsselung, der Art von Verschlüsselung, die WhatsApp, Signal und Apples iMessage verwenden, um sicherzustellen, dass nur der Absender und der beabsichtigte Empfänger der Daten Zugriff auf die betreffende Kommunikation haben. Und es ist nicht nur das FBI, das sich für die Beschränkung der Verschlüsselung einsetzt. Indien, China, das Vereinigte Königreich - das von China gelobt wurde, als dieses sein eigenes Ge-

Original

In the U.S., Senators Burr and Feinstein have recently drafted the Compliance with Court Orders Act of 2016, which could be introduced at any time - to disastrous consequences. It will likely lead to greater crime, more compromised information, and both more prosecutions and possibly deaths of journalists and activists in repressive countries. What this and other mandates sought and will not do, however, is limit the use of encryption by terrorists and criminals. These actors - to whom that we most want to limit the use of tools that law enforcement cannot gain access to - will still have available to them open source tools, tools that they developed themselves as well as tools developed in other countries to which jurisdiction does not reach. It will only have a primary impact of limiting the amount of security available to everyday citizenry, including the most at-risk users.

And finally, a word on government hacking, because both the FBI and the NSA have entire units devoted to government hacking. And the FBI is now seeking a rule change, in fact, a rule change that will go into effect at the beginning of December of this year, unless Congress acts. So, they have switched the presumption: Congress does not have to act to change the rule; they simply have to do nothing, and the change goes into effect. Senator Wyden is on the floor of the U.S. Congress, I believe, today in order to try to pass legislation that would stop this change, with the Stopping Mass Hacking Act. But the ability for Congress to act this year, because of the U.S. elections, is going to be limited. And the rule change will ostensibly give the FBI

Deutsche Übersetzung

setz zur Beschränkung von End-to-End-Verschlüsselung verabschiedete - sowie, leider, auch Frankreich und Deutschland setzen sich für die Beschränkung der Verschlüsselung ein - sowohl ihrer Entwicklung als auch ihrer Nutzung.

In den USA haben die Senatoren Burr und Feinstein kürzlich den Entwurf für einen Compliance with Court Orders Act of 2016 [Gesetz von 2016 zur Einhaltung von gerichtlichen Anordnungen] verfasst, der jederzeit - mit verheerenden Folgen - verabschiedet werden könnte. Das Gesetz wird wahrscheinlich zu mehr Kriminalität, mehr kompromittierenden Informationen sowie mehr Verfolgung und Todesfällen von Journalisten und Aktivisten in repressiv regierten Ländern führen. Was diese und auch andere Bestimmungen erreichen wollen, aber nicht werden, ist, die Nutzung von Verschlüsselung durch Terroristen und Kriminelle zu beschränken. Diese Akteure - deren Nutzung von Werkzeugen, auf die die Strafverfolgungsbehörden keinen Zugriff haben, wir am meisten beschränken wollen - verfügen weiterhin über Open-Source-Werkzeuge, Werkzeuge, die sie selbst entwickelt haben, und Werkzeuge, die in anderen Ländern entwickelt werden, in denen unsere Gesetze nicht gelten. Mehr als alles andere wird es weniger Möglichkeiten zur Absicherung für den Normalbürger, einschließlich der am meisten gefährdeten User, bringen.

Und zum Abschluss ein paar Worte zum Thema staatliches Hacking, denn sowohl das FBI als auch die NSA haben ganze Einheiten, die sich ausschließlich dem Hacken für die Regierung widmen. Und das FBI bemüht sich nun um eine Regeländerung, und zwar eine Regeländerung, die Anfang Dezember dieses Jahres in Kraft tritt, wenn der Kongress nicht handelt. Sie haben die Voraussetzung geändert: Der Kongress muss nicht aktiv werden, um die Regel zu ändern. Sie müssen einfach gar nichts tun, und die Änderung tritt in Kraft. Senator Wyden steht, glaube ich, heute vor dem Kongress, um zu versuchen, die Änderung mit einem Gesetz, dem Stopping Mass Hacking Act [Gesetz zum Stopp des massenhaften Hackings] zu stoppen. Jedoch wird die

Original

authority to hack into computers around the world, so long as they don't know where the computer is located. Right now, the FBI has no substantive authority under U.S. law to hack; in fact, Congress has never spoken to this issue in U.S. law.

So, nobody really knows how the FBI is engaged in this activity. There is very little transparency about their operations or the safeguards that they have in place. Earlier this week, Access Now published a report called "A Human Rights Response to Government Hacking", where we ask for a presumptive prohibition on government hacking as well as more transparency and ten safeguards that need to be in place if hacking does occur. We hope that Congress will take this opportunity to examine government hacking, to look at what safeguards need to be in place, and to actually pass a law with meaningful safeguards and limitations. But that law does not yet exist, and so hacking is occurring and compromising the security of everybody.

And one last thing before I close: I want to emphasize that surveillance is not only a problem in the United States. The focus on the United States is proper, in that the U.S. government devotes more resources, both time and money, to implementing surveillance authorities. However, governments globally are taking steps to increase their surveillance authority and power without due regard for human rights or for a potential for abuse. It is becoming trivially easy, both in terms of law and technology, to collect more information about a person than that person is even aware exists, to actually collect so much information that you can make predictions about

Deutsche Übersetzung

Handlungsfähigkeit des Kongresses in diesem Jahr aufgrund der US-Wahlen begrenzt sein. Und die Regeländerung wird dem FBI augenscheinlich die Vollmacht geben, sich in Computer überall auf der Welt zu hacken, solange es nicht weiß, wo der Computer sich befindet. Aktuell hat das FBI unter US-Recht keine substanzielle Vollmacht zum Hacken. Tatsächlich hat der Kongress über diese Frage im US-Recht überhaupt nie gesprochen.

So weiß also niemand, wie die Aktivitäten des FBI diesbezüglich aussehen. Hinsichtlich ihrer Operationen oder den von ihm eingerichteten Sicherheitsvorkehrungen herrscht sehr wenig Transparenz. In dieser Woche hat Access Now einen Bericht mit dem Titel „A Human Rights Response to Government Hacking" [„Eine Antwort von Menschenrechtlern auf staatliches Hacking"] veröffentlicht. Darin fordern wir ein mutmaßliches Verbot des staatlichen Hackings sowie mehr Transparenz und zehn Sicherheitsvorkehrungen, die eingerichtet sein müssen, wenn Hacking zur Anwendung kommt. Wir hoffen, dass der Kongress diese Gelegenheit nutzt, staatliches Hacking zu überprüfen, zu untersuchen, welche Sicherheitsvorkehrungen eingerichtet sein müssen, und ein Gesetz zu verabschieden, das sinnvolle Sicherheitsvorkehrungen und Beschränkungen vorschreibt. Aber ein solches Gesetz existiert noch nicht. Und deswegen findet das Hacking statt und beeinträchtigt die Sicherheit aller.

Noch eine letzte Sache, bevor ich zum Schluss komme: Ich möchte betonen, dass Überwachung nicht nur in den USA ein Problem ist. Allerdings ist der Fokus auf die USA insofern angemessen, als die US-Regierung zur Einrichtung von Überwachungsvollmachten einen höheren finanziellen und zeitlichen Aufwand betreibt. Jedoch sind Regierungen weltweit dabei, ihre Überwachungsvollmachten und -möglichkeiten auszubauen, ohne dabei Menschenrechte oder potenziellen Missbrauch in gebührender Weise zu beachten. Es wird sowohl technisch als auch rechtlich geradezu lächerlich einfach, mehr Daten über eine Person zu sammeln, als dieser Person

Original

who that person will be and what he will do in the future.

As such, my final call to action is for Germany to lead in a global conversation about how to curb these practices and end the global surveillance arms race. We must move toward a recognition of privacy as a right to be protected and not a limit to be challenged.

Thank you. And I look forward to your questions.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank, Frau Stepanovich, für Ihre Ausführungen, und ganz herzlichen Dank an alle Mitglieder des Panels, an alle Sachverständigen. Manchmal habe ich mich ein wenig erinnert gefühlt an unsere Sachverständigenanhörungen zu den technischen Dingen, insbesondere bei den Ausführungen von Chris Soghoian. Mehr Verschlüsselung als ein Instrument, um Datensicherheit zu erzielen, der zu laxe Umgang mit den eigenen Daten - das hat mich schon ein bisschen erinnert an das, was wir von anderen Experten sehr zu Anfang dieses Ausschusses gehört haben.

Wir würden jetzt übergehen zu den Fragen der Abgeordneten. Vorab: Wenn Sie eine Pause brauchen - wir werden sowieso nach einiger Zeit eine Pause machen -, wenn nicht ausreichend Kaffee, Getränke etc. da sind, geben Sie ein kurzes Zeichen. Sie sollen sich bei uns wohlfühlen.

Ich würde mit einer kleinen Eingangsfrage beginnen und dann aber auch das Wort an die Kolleginnen und Kollegen weitergeben. - Ich hätte zwei Fragen jeweils, also die gleiche Frage an Mr. Halperin und Ms. Stepanovich. Und die Frage wäre eigentlich ganz allgemein.

Deutsche Übersetzung

selbst bekannt sind, und so viele Daten zu sammeln, dass sich daraus Voraussagen darüber treffen lassen, wer diese Person sein wird und was sie in Zukunft tun wird.

Daher lautet mein abschließender Appell an Deutschland, eine weltweite Debatte darüber anzuführen, wie man diese Praktiken eindämmen und das weltweite Überwachungswettrüsten beenden kann. Wir müssen erreichen, dass Privatsphäre als ein Recht anerkannt wird, das geschützt werden muss, und keine Grenze ist, die sich verschieben lässt.

Vielen Dank. Ich freue mich auf Ihre Fragen.

Original

Sachverständige Amie Stepanovich: Excuse me, Dr. Sensburg. Could we actually get a break now before the questions begin?

Vorsitzender Dr. Patrick Sensburg: Right now? Okay. We can have five minutes, ten minutes or - -

Sachverständiger Dr. Christopher Soghoian: Sure.

Sachverständige Ashley Gorski: Five is fine.

Vorsitzender Dr. Patrick Sensburg: Then we're going to take a ten-minute break. Is it enough?

Sachverständige Ashley Gorski: Yes.

Vorsitzender Dr. Patrick Sensburg: So, a ten-minute break before we start. Thank you. - Dann ist die Sitzung für zehn Minuten unterbrochen.

(Unterbrechung von
13.37 bis 13.47 Uhr)

Vorsitzender Dr. Patrick Sensburg: Wir setzen die unterbrochene Sitzung des 1. Untersuchungsausschusses fort. Ich freue mich, dass Sie wieder da sind. Auch für die Zukunft geben Sie ein kurzes Zeichen für eine Pause, dann machen wir das natürlich auch immer.

Zwei Fragen meinerseits zum Einstieg, und dann kommen die Kolleginnen und Kollegen. Es ist die gleiche Frage jeweils, einmal an Mr. Halperin und einmal an Amie Stepanovich. Mich würde interessieren: Was erwarten und erhoffen Sie sich denn von diesem Ausschuss an Erkenntnissen, möglicherweise an Unterstützung beim Einsatz für den Umgang, für einen sicheren Umgang, für einen geschützten Umgang mit unser aller Daten, mit Privatheit, natürlich bei gleichzeitiger Aufrechterhaltung der Arbeitsfähigkeit der Sicherheitsbehörden? Was ist Ihre

Deutsche Übersetzung

Sachverständige Amie Stepanovich: *Entschuldigen Sie, Dr. Sensburg. Könnten wir vielleicht eine Pause machen, bevor wir mit den Fragen beginnen?*

Vorsitzender Dr. Patrick Sensburg: *Jetzt sofort? Okay. Wir können fünf Minuten machen, zehn Minuten oder - -*

Sachverständiger Dr. Christopher Soghoian: *Natürlich.*

Sachverständige Ashley Gorski: *Fünf ist gut.*

Vorsitzender Dr. Patrick Sensburg: *Dann machen wir eine zehnminütige Pause. Ist das genug?*

Sachverständige Ashley Gorski: *Ja.*

Vorsitzender Dr. Patrick Sensburg: *Also, zehn Minuten Pause, bevor wir beginnen. Danke. - Dann ist die Sitzung für zehn Minuten unterbrochen.*

Original

Erwartung an diesen Ausschuss? Vielleicht können wir uns dann auch so ein bisschen danach richten, gemeinsam zusammenzuarbeiten. Also, Ihre Erwartungshaltung, warum Sie heute hier sind, würde ich gerne wissen. - Machen wir „ladies first“? - Frau Stepanovich.

Sachverständige Amie Stepanovich: Thank you very much. - I think the primary expectation that we have for all governments, including that in Germany, is to effectively implement what we call the “International Principles on the Application of Human Rights to Communications Surveillance”. This is a set of 13 principles that has been agreed to by organizations and some governments around the world, available at necessaryandproportionate.org, that we believe represent what is currently written already into human rights law and policy - both through court findings, policy documents, and generally understood interpretations of law.

Access Now has published an implementation guide on what we think laws that adequately protect human rights would look like under those principles - so trying to engage in a realistic conversation about to what extent and how laws can be passed that protect human rights, that provide for adequate notice to users about when they can be subject to surveillance, both users within Germany and users around the world, and then to provide a common standard for both to make sure that extraterritorial surveillance does not happen in a way that violates other users’ rights or that undermines Internet security globally.

Vorsitzender Dr. Patrick Sensburg: Okay. Ganz herzlichen Dank. - Mr. Halperin, was sind Ihre Erwartungen ganz konkret an diesen Ausschuss?

Sachverständiger Dr. Morton H. Halperin: My hope is that you will say that, having started out being concerned about what the United States

Deutsche Übersetzung

Sachverständige Amie Stepanovich: *Vielen Dank. Ich denke, vorrangig erwarten wir von allen Regierungen, auch der deutschen, die Umsetzung der sogenannten Internationalen Grundsätze für die Anwendung der Menschenrechte in der Kommunikationsüberwachung. Dabei handelt es sich um dreizehn Grundsätze, die von Unternehmen und einigen Regierungen weltweit vereinbart wurden und die unter necessaryandproportionate.org online einzusehen sind. Unserer Ansicht nach spiegeln diese Grundsätze das wider, was bereits in der Menschenrechtsgesetzgebung und -politik festgeschrieben ist, in Form von Gerichtsurteilen, Strategiepapieren und auch allgemein üblichen Rechtsauslegungen.*

Access Now hat einen Umsetzungsleitfaden herausgebracht, in dem wir darlegen, wie diesen Grundsätzen zufolge Gesetze aussehen müssten, die die Menschenrechte angemessen schützen. Wir möchten damit einen realistischen Diskurs darüber anregen, wie und in welchem Maß Gesetze erlassen werden können, die die Menschenrechte schützen, die Nutzer sowohl in Deutschland als auch in der ganzen Welt angemessen darüber informieren, ob und wann sie möglicherweise überwacht werden, und die außerdem einen gemeinsamen Standard für beide Gruppen festlegen, um sicherzustellen, dass eine extraterritoriale Überwachung nicht gegen die Rechte anderer Nutzer verstößt oder die globale Internetsicherheit gefährdet.

Sachverständiger Dr. Morton H. Halperin: *Meine Hoffnung besteht darin, dass Sie nach Ihren ursprünglichen Bedenken hinsichtlich des*

Original

government was doing in terms of spying on Germans, you discovered that you also need to be worried about what the German government is doing, and the U.K. government, and the French government as well as, of course, the Russians and the Chinese. But, as I say, that's a separate problem.

And then my hope is that you will say that, given our desire to not have these problems intrude on the privacy of our citizens, but also on the cooperative nature of the Internet and the process of sharing information, the only solution to the problem is one that goes beyond Europe and that involves the United States and other like-minded countries in coming together on a set of agreed principles, which then get translated into legislation. I would myself spend less time arguing about whether the necessary and proper provisions actually exist in the law and what they actually mean, because if you could pass a magic wand and make the U.S. government obey those principles, it would tell you that it already does so. And the problem is, I think, they're at a level of generality that they would say that, Fine, we accept these principles. Now we do exactly what we've done before.

So, I would much rather argue about what actually needs to be done. What are the six categories of kinds of information that you can collect about private citizens? How do we make sure that you don't collect other kinds and deal in a very concrete way with the notion that you can protect the security of countries, and you can protect the security of all of our countries, while still respecting the privacy rights of private citizens? We haven't done it, because nobody has thought it was important or an important principle, and because intelligence agencies tend to always err on the side of collecting more. And

Deutsche Übersetzung

Ausspionierens von Deutschen durch die Regierung der USA erkannt haben, dass Sie auch über die Aktivitäten der deutschen Regierung besorgt sein müssen, ebenso wie die der britischen, der französischen und natürlich auch der russischen und chinesischen Regierungen. Aber das ist, wie gesagt, ein anderes Problem.

Ferner habe ich die Hoffnung, dass Sie dann sagen, dass - angesichts der Tatsache, dass wir nicht möchten, dass diese Probleme die Privatsphäre unserer Bürger sowie auch die kooperative Natur des Internets und die gemeinsame Nutzung von Informationen einschränken - die einzig mögliche Lösung dieses Problems eine ist, die über Europa hinausgeht und auch die USA sowie weitere, gleichgesinnte Länder einschließt und darin besteht, dass alle gemeinsam eine Reihe von Grundsätzen vereinbaren, die dann in die jeweilige Gesetzgebung übertragen werden. Ich persönlich würde weniger Zeit dafür aufwenden, darüber zu streiten, ob die bestehenden Gesetze bereits die notwendigen und angemessenen Regelungen enthalten und was sie überhaupt bedeuten; denn wenn man einen Zauberstab hätte und die Regierung der USA zwingen könnte, diese Grundsätze einzuhalten, dann würde sie erklären, dass sie dies bereits tut. Das Problem liegt meiner Meinung nach darin, dass die Grundsätze so allgemein gefasst sind, dass die Regierung einfach sagen würde: Gut, wir bekennen uns zu diesen Grundsätzen. Und jetzt machen wir genau so weiter wie zuvor.

Darum würde ich sehr viel lieber darüber sprechen, was tatsächlich zu tun ist. Welches sind die sechs Datenkategorien, die über Privatpersonen erfasst werden können? Wie können wir sicherstellen, dass nicht weitere Datenarten erfasst werden, und wie gehen wir ganz konkret mit dem Konzept um, die Sicherheit von Ländern, die Sicherheit aller unserer Länder zu schützen, ohne dabei gegen die Persönlichkeitsrechte von Privatbürgern zu verstoßen? Wir haben das nicht getan, weil niemand es für wichtig oder einen wichtigen Grundsatz hielt und weil Geheimdienste immer dazu neigen, lieber mehr

Original

therefore governments - democratic governments - have to take responsibility for this and come together and say, We give the parameters to the intelligence agencies, and these parameters will both protect our security and protect our privacy.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich hatte als erste Meldung, glaube ich, Frau Kollegin Renner gesehen - also ich nicht, aber das Ausschusssekretariat. Da bin ich mir ziemlich sicher, die sind aufmerksam. - Ja, genau. Danach Herr Kollege Flisek. - Frau Kollegin Renner.

Martina Renner (DIE LINKE): Danke, Herr Vorsitzender. - Meine erste Frage würde ich gerne an Frau Gorski richten. Wir haben ja jetzt übereinstimmend durch Sie gehört, dass ein Ergebnis der Snowden-Veröffentlichungen war, dass zu den Schutzrechten der US-Bürger und -Bürgerinnen nun auch Bürger und Bürgerinnen bestimmter Länder auch vor Überwachung, insbesondere Massenüberwachung, geschützt werden sollen. Sie haben aber auf die Problematik hingewiesen, wie schwierig es ist, als ziviler Kläger oder Klägerin tatsächlich gerichtlich klären zu lassen, ob diese Überwachung gerechtfertigt war und möglicherweise ja auch aus solchen Sprüchen dann Schlussfolgerungen zu ziehen sind hinsichtlich der Löschung der Dateien.

Wie sieht es denn mit den Schutzrechten von Nicht-US-Bürgern und -Bürgerinnen jetzt aus? Welche Rechtswege stehen diesen offen? Gibt es die Möglichkeit, Auskunft zu verlangen, welche meiner Daten in den USA verarbeitet wurden? Habe ich Anspruch darauf, Beschwerde zu erheben gegen diese Datensammlung? Und besteht zum Beispiel auch die Möglichkeit, dann Daten löschen zu lassen? - Das wäre meine Frage an Sie.

Dann habe ich eine zweite Frage. Da bitte ich einfach den oder die, der oder die sich kompetent oder angesprochen fühlt, zu antworten.

Deutsche Übersetzung

als weniger Daten zu erfassen. Und darum müssen die Regierungen - demokratische Regierungen - hier die Verantwortung übernehmen und sich zusammensetzen, um den Geheimdiensten Parameter an die Hand zu geben, und diese Parameter werden sowohl unsere Sicherheit als auch unsere Persönlichkeitsrechte schützen.

Original

Mich würde interessieren: Bei diesen ganzen Schutzrechten und Vorkehrungen, die jetzt auch nach den Snowden-Veröffentlichungen eingezogen wurden, geht es ja auch immer um die Frage: Was sind personenbezogene bzw. personenbeziehbare Daten? Insbesondere die Metadatenproblematik spielte da eine große Rolle. Ich möchte gerne wissen, wie weit der Schutzrahmen mittlerweile geht.

Sind neben Inhaltsdaten und Metadaten auch solche Informationen geschützt, die zum Beispiel aus sozialen Netzwerken erhoben werden, also indem zum Beispiel mit Bilderkennungssoftware dort gearbeitet wird oder Ähnliches? Wie sieht es mit kryptierten Verkehren aus? Werden diese erfasst und gespeichert, um sie vielleicht in Zukunft entschlüsseln und dann auch verarbeiten zu können und Ähnliches? Also, wie weit sind alle Arten für uns vorstellbarer Daten und Dateien tatsächlich durch diese Schutzrechte umfasst?

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Also, die erste Frage, völlig klar, ging an Ashley Gorski.

Sachverständige Ashley Gorski: Thank you very much for your question. - At the outset, I would just note that there's a significant conceptual problem here. Because if, as a non-U.S. person, you want to come into court - setting aside arguments about what substantive rights you may have in court - at the outset, you, in the ordinary course, will not be notified of the fact that your information in particular was subject to bulk surveillance, or targeted surveillance, or bulk searching, or any other collection, retention, dissemination, use. In the ordinary course, with respect to foreign intelligence surveillance, this notice is lacking.

Now, if the United States government is proceeding against you in the context of a criminal hearing or an administrative proceeding, you may be notified, under certain

Deutsche Übersetzung

Sachverständige Ashley Gorski: *Vielen Dank für diese Frage. Zunächst möchte ich anmerken, dass hier ein bedeutendes konzeptionelles Problem vorliegt. Denn wenn Sie als Nicht-US-Person vor Gericht kommen wollen - die Frage, welche materiellen Rechte Sie möglicherweise vor Gericht haben, mal außen vor gelassen -, werden Sie im üblichen Verlauf nicht zu Beginn darüber informiert, dass Ihre speziellen Daten Gegenstand einer massenhaften Überwachung, einer gezielten Überwachung, einer Massensuche oder irgendeiner anderen Erfassung, Vorratsspeicherung, Verbreitung oder Nutzung waren. Im normalen Verfahren fehlt dieser Hinweis in Bezug auf die Überwachung in der Auslandsaufklärung.*

Wenn nun die US-Behörden im Rahmen eines Straf- oder Verwaltungsverfahrens gegen Sie vorgehen, werden Sie darüber in Kenntnis gesetzt, dass Beweismittel, die die Regierung gegen Sie

Original

surveillance authorities, that some evidence that the government wants to use against you was obtained or derived from that surveillance. But, as I mentioned during my testimony, the government has a very narrow interpretation of its notice obligation in the criminal context. So in the civil context, in the ordinary course, without notice, you would lack standing - or, at least, there's a very good chance that you would lack standing - to bring suit.

We are currently representing Wikimedia, owner and operator of Wikipedia, which is one of the ten most visited websites in the world, as well as seven other legal, media and educational organizations in a challenge to Upstream surveillance under Section 702. And the district court held, in our case, that Wikimedia lacked standing, and the other plaintiffs lacked standing to challenge Upstream surveillance, because they could not show with sufficient certainty that their communications had been subject to surveillance. That case is pending on appeal, but it just illustrates the difficulty of getting over the standing hurdle. And without notice of the foreign intelligence surveillance, it's very difficult to establish standing and that's even setting aside the questions about what substantive rights you would have as a non-U.S. person in a U.S. court.

One other doctrine that I think bears emphasis and is worth mentioning here is what's known as the "state secrets doctrine". So, in cases involving information that the U.S. government deems a state secret, if the government argues that it cannot defend the case without making that information public or known, then it can ask the court to dismiss the case altogether under this state secrets doctrine. It's an incredibly blunt instrument to foreclose and forestall litigation and prevent reaching the merits of whether this surveillance is in fact lawful.

Deutsche Übersetzung

zu verwenden beabsichtigt, von bestimmten Überwachungsbehörden erfasst oder von den Ergebnissen der Überwachung abgeleitet wurden. Doch wie ich bereits in meiner vorausgehenden Einlassung erwähnte, folgt die Regierung einer sehr eingeschränkten Auslegung, was ihre Informationspflicht im Rahmen von Strafverhandlungen betrifft. Im zivilrechtlichen Rahmen würden Sie also im Regelfall ohne diese Information keine ausreichende Grundlage für eine Klage haben, oder zumindest ist es sehr wahrscheinlich, dass Sie keine ausreichende Grundlage hätten.

Wir vertreten gegenwärtig Wikimedia, den Besitzer und Betreiber von Wikipedia, einer der zehn weltweit meistbesuchten Websites, ebenso wie sieben andere juristische, Medien- und Bildungsorganisationen in ihrer Klage gegen die Upstream-Überwachung gemäß § 702. Und das Bezirksgericht entschied in unserem Fall, dass Wikimedia und die anderen Kläger keine ausreichenden Beweise für eine Klage gegen die Upstream-Überwachung haben, weil sie nicht mit hinreichender Sicherheit belegen konnten, dass ihre Internetkommunikation von der Überwachung betroffen war. Das Berufungsverfahren ist derzeit anhängig, aber es zeigt, wie schwierig es ist, diese Hürde der Klageabweisung wegen unzureichender Beweise zu überwinden. Ohne In-Kenntnis-Setzung über die Überwachung in der Auslandsaufklärung es ist sehr schwierig, ausreichende Beweise für eine Klage vorzulegen, ganz abgesehen von der Frage, welche materiellen Rechte man als Nicht-US-Person vor einem Gericht der Vereinigten Staaten hätte.

Eine weitere Doktrin, die ich an dieser Stelle hervorheben möchte und die erwähnenswert ist, ist die sogenannte Staatsgeheimnis-Doktrin. Betrifft ein Verfahren Informationen, die die US-Regierung als Staatsgeheimnis betrachtet, so kann sie das Gericht auffordern, das Verfahren gemäß der Staatsgeheimnis-Doktrin einzustellen, weil sie die betreffenden Ansprüche nicht abwehren kann, ohne diese Informationen öffentlich bzw. bekannt zu machen. Dies ist ein unglaublich plumpes Mittel zur Einstellung und Verhinderung von Gerichtsverfahren, mit dem

Original

And I don't know if anyone else wants to elaborate on the Judicial Redress Act or other modes of redress of non-U.S. persons.

Sachverständiger Dr. Christopher Soghoian: Her second question was a tech question, right?

Sachverständiger Dr. Morton H. Halperin: What is personal data?

Sachverständiger Dr. Christopher Soghoian: No, I thought it was about what technology protects metadata.

Vorsitzender Dr. Patrick Sensburg: Die zweite Frage wäre nach personenbezogenen Daten und dem Schutzrahmen gewesen. Es wäre wahrscheinlich ein juristischer Schwerpunkt in der Frage, wenn ich das richtig sehe.

Martina Renner (DIE LINKE): Auch ein technischer.

Vorsitzender Dr. Patrick Sensburg: Ja, technisch, juristisch. Also, bei Technik ist es Herr Soghoian. Bitte schön.

Sachverständiger Dr. Christopher Soghoian: So let me try and explain as best I can. You asked about what protections there are for metadata and for encrypted information. The technology community has a lot more experience trying to protect the contents of communications. And now there are technologies available to the public, to businesses and to governments that can allow you to protect the contents of your telephone calls, the contents of your text messages, the contents of your web browsing. In some cases it is up to the user to choose and to use those technologies; in some cases it is up to the companies that provide you with services. So if Google or WhatsApp or Facebook decide to turn on the technology, then your information can be

Deutsche Übersetzung

auch die Klärung verhindert wird, ob diese Überwachung überhaupt rechtmäßig ist.

Ich weiß nicht, ob jemand anders noch Genaueres zum Judicial Redress Act oder anderen Formen der Entschädigung für Nicht-US-Personen sagen möchte.

Sachverständiger Dr. Christopher Soghoian: *Ihre zweite Frage bezog sich auf die Technologie, richtig?*

Sachverständiger Dr. Morton H. Halperin: *Was sind personenbezogene Daten?*

Sachverständiger Dr. Christopher Soghoian: *Nein, ich dachte, es ging darum, welche Technologien zum Schutz von Metadaten es gibt.*

Sachverständiger Dr. Christopher Soghoian: *Lassen Sie mich versuchen, das Ganze so gut ich kann zu erklären. Sie fragten, welchen Schutz es für Metadaten und verschlüsselte Informationen gibt. Die Technologiebranche hat sehr viel mehr Erfahrung darin, Kommunikationsinhalte zu schützen. Mittlerweile gibt es auch Technologien, die für die allgemeine Öffentlichkeit ebenso wie für Unternehmen und Regierungen zugänglich sind und mit denen man die Inhalte von Telefongesprächen, SMS-Nachrichten und Surfaktivitäten im Internet schützen kann. In manchen Fällen liegt die Entscheidung für solche Technologien und ihre Nutzung beim Nutzer, in anderen wird sie durch die Unternehmen getroffen, die dem Nutzer Dienste bereitstellen.*

Original

protected. And, certainly, as I described in my oral testimony, there has been a trend towards the use of encryption technology that protects the contents of conversations.

The technology community does not have as much experience in creating technologies that are designed to protect the metadata. So we can protect the "what", but not the "when" and the "who". Now, if you're sending an email to a colleague then the contents of that conversation is the important thing. But if you're making a telephone call to a suicide hotline or to an abortion clinic, then the "when" and the "who" is probably just as important as the "what". We desperately need more research into technologies that protect metadata. This is an area of active research by the tech community; it's something that both the U.S. and European governments are funding, and I would strongly encourage you to continue funding research into potential metadata protection technologies. There are technologies that are available now that can let you protect, for example, the metadata around instant messages, or the metadata around web browsing. But we desperately need more research.

You also asked, Well, what are the retention rules for encrypted data? - We know from some of the Snowden documents that were published by *The Guardian* that the NSA's own data retention rules do not apply to encrypted data. This sort of creates this ironic situation where the least sensitive data in our lives, which is probably not encrypted, has a mandatory data retention period, I think, of five years. And then the most sensitive data - our health records, our email, our social network browsing, our deeply personal and private information, which is encrypted - can then be effectively indefinitely retained by the NSA.

Deutsche Übersetzung

Wenn also Google oder WhatsApp oder Facebook entscheiden, eine Technologie einzusetzen, dann können die Informationen des Nutzers geschützt werden. Und es gibt, wie ich in meiner mündlichen Aussage beschrieben habe, einen Trend zur Nutzung von Verschlüsselungstechnologien, die Kommunikationsinhalte schützen.

In der Entwicklung von Technologien zum Schutz von Metadaten ist die Technologiebranche weniger erfahren. Wir können also das Was schützen, nicht jedoch das Wann und Wer. Wenn Sie einem Kollegen eine E-Mail schicken, dann ist der Inhalt dieser Kommunikation das Wichtige. Wenn Sie jedoch bei einer Suizid-Hotline oder einer Abtreibungspraxis anrufen, dann ist das Wann und Wer wahrscheinlich ebenso wichtig wie das Was. Wir benötigen unbedingt mehr Forschung zu Technologien, durch die sich Metadaten schützen lassen. Die Technologiebranche forscht hier aktiv, die US-Regierung ebenso wie europäische Regierungen unterstützen die Forschung, und ich möchte Ihnen dringend ans Herz legen, die Forschung nach möglichen Technologien zum Schutz von Metadaten auch weiterhin zu fördern. Es gibt heute verfügbare Technologien, mit denen man zum Beispiel die Metadaten im Zusammenhang mit Instant Messaging oder Websurfen schützen kann. Aber wir brauchen hier dringend weitere Forschung.

Sie fragten auch nach den Bestimmungen zur Speicherung verschlüsselter Daten. Aus den vom Guardian veröffentlichten Snowden-Dokumenten wissen wir, dass die Bestimmungen über Datenspeicherung der NSA nicht für verschlüsselte Daten gelten. Dadurch ergibt sich die leicht bizarre Situation, dass für die am wenigsten sensiblen Daten in unserem Leben, die wahrscheinlich nicht verschlüsselt sind, eine Aufbewahrungsfrist von, ich glaube, fünf Jahren gilt, während die sensibelsten Daten - unsere Gesundheitsdaten, unsere E-Mails, unsere Aktivitäten in sozialen Netzwerken, all die persönlichen und vertraulichen Daten, die verschlüsselt sind - quasi unbefristet von der NSA gespeichert werden können.

Original

The reason the NSA waives its retention and data destruction rules for encrypted data is sort of twofold: One, NSA hopes that, over time, they will develop the capability to decrypt the data because of advancements in computing - so, over time, computers get faster, NSA will develop the ability to attack encryption algorithms - or, NSA will steal the encryption keys if they are held by third parties. So, for example, last year *The Intercept* revealed that GCHQ had hacked into Gemalto - the French-Dutch manufacturer of SIM cards - and stolen many of the SIM card encryption keys used by Gemalto. In that case, with those encryption keys in its possession, GCHQ could decrypt, after the theft, conversations that had been previously recorded and saved in encrypted form.

And so we should not just be worried about the capabilities of the NSA and GCHQ and other intelligence services today; if they are retaining data of encrypted communications now, they may be able to decrypt it five years, or ten years, or twenty years into the future. And that is one of the reasons why the technology community is so focused right now on the development of what are called "post-quantum" encryption algorithms - encryption algorithms that can protect our communications from advancements in computing that may be available in five or ten years.

Vorsitzender Dr. Patrick Sensburg: Okay. - Ich gucke nur mal zur Frau Kollegin Renner. - Danke schön. - Dann kommen wir zur nächsten Frage, die stellt der Kollege Flisek.

Christian Flisek (SPD): Danke, Herr Vorsitzender. - Herr Edgar, ich würde Sie, nachdem Sie sich ja in Ihrem Eingangsstatement starkgemacht haben dafür - mit einigen anderen auch, deren Stellungnahmen in dieselbe Richtung gingen -,

Deutsche Übersetzung

Die NSA wendet ihre Bestimmungen über die Datenspeicherung und -vernichtung aus zwei Gründen nicht auf verschlüsselte Daten an. Erstens hofft man bei der NSA, dass man im Laufe der Zeit in der Lage sein wird, diese Daten zu entschlüsseln, weil die Computertechnologie entsprechende Fortschritte macht - dass also die NSA zukünftig mit schnelleren Computern in der Lage sein wird, die Verschlüsselungsalgorithmen zu knacken. Oder sie stehlen die Verschlüsselungsschlüssel, falls diese im Besitz von Dritten sind. So enthüllte [die Website] „The Intercept" beispielsweise im vergangenen Jahr, dass sich der britische Geheimdienst GCHQ in das Netz des französisch-niederländischen SIM-Kartenherstellers Gemalto gehackt und zahlreiche der von Gemalto verwendeten SIM-Karten-Schlüssel gestohlen hatte. Nach dem Diebstahl dieser Verschlüsselungsschlüssel konnte das GCHQ Gespräche entschlüsseln, die bereits vorher verschlüsselt aufgezeichnet und gespeichert worden waren.

Wir sollten uns also nicht nur Gedanken darüber machen, wozu NSA und GCHQ und andere Geheimdienste heute in der Lage sind, denn wenn sie heute verschlüsselte Kommunikationsdaten speichern, können sie diese vielleicht in fünf, zehn oder zwanzig Jahren entschlüsseln. Und dies ist einer der Gründe, weshalb die Technologiebranche sich zurzeit so intensiv mit der Entwicklung von sogenannten Post-Quanten-Verschlüsselungsalgorithmen beschäftigt - also mit Verschlüsselungsalgorithmen, die unsere Kommunikation vor der Entschlüsselung durch Computer schützen, die in vielleicht fünf oder zehn Jahren verfügbar sind.

Original

dass wir versuchen, gerade bei der Frage der Ausland-Ausland-Verkehre, also bei der Frage, wie Geheimdienste die jeweiligen Ausländer behandeln, da zu internationalen Standards zu kommen, gerne mal fragen - ganz offen gesprochen, gerade jetzt mal im Verhältnis USA-Europa oder vielleicht auch im bilateralen Verhältnis USA-Deutschland -: Wie realistisch schätzen Sie denn das überhaupt ein, dass es für solche Standards, die auch Substanz haben, die eine bestimmte Qualität haben, dass es für so etwas auch tatsächlich eine politische Mehrheit und einen politischen Willen geben könnte? Und sehen Sie das Ganze dann tatsächlich eher auf der Ebene eines internationalen völkerrechtlichen Vertrages verortet oder eher auf der Ebene bilateraler Verhandlungen?

In diesem Zusammenhang würde ich Sie auch gerne fragen: Wir hatten ja, als die Snowden-Veröffentlichungen hier in Deutschland auftauchten, eine Debatte darüber, dass die Bundesrepublik Deutschland gegebenenfalls mit den Vereinigen Staaten ein sogenanntes No-Spy-Abkommen abschließt. War das jemals aus Ihrer persönlichen Bewertung, aus Ihrer Fachexpertise eine realistische Option auch im Hinblick darauf, dass es solche Abkommen vielleicht zwischen den USA und anderen Ländern bereits gibt? - Also, das wäre meine Frage an Sie.

An Frau Gorski hätte ich gerne die Frage gestellt: Wir haben als Untersuchungsausschuss ja hier den Zeitraum zwischen 2001 - wir haben den ja bewusst dort gelegt, weil wir 9/11 eben für eine entsprechende Zäsur halten - bis zu den Snowden-Veröffentlichungen vor Augen. Das ist also eine ganze Zeitspanne, in der sich auch in der technischen Entwicklung sehr viel getan hat. Was wir jetzt hier im Untersuchungsausschuss aufgearbeitet haben, sind die offiziellen, ich sage das mal, uns bekannten Kooperationsprojekte zwischen US-Diensten, namentlich der NSA, und unserem Auslandsgeheimdienst. Aber wie würden Sie, wenn wir uns die Frage stellen „Was machen eigentlich US-Geheimdienste in Bezug auf Deutschland, und wie viel davon findet dann eigentlich außerhalb von offiziellen

Deutsche Übersetzung

Original

Kooperationsprojekten statt?“, ohne dass Sie wahrscheinlich jetzt valide empirische Ergebnisse vorliegen haben, dieses Verhältnis einschätzen? Also, wenn man sagt: „nachrichtendienstliche Tätigkeit in Bezug auf ein Land wie Deutschland“, was davon findet sozusagen außerhalb jeder Kooperation statt?

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Die erste Frage ging an Herrn Edgar.

Sachverständiger Timothy H. Edgar: I thank you very much, Mr. Flisek. - So I think we would start with: What is the baseline of protection extended by Presidential Policy Directive 28 to all citizens? And then we should also think about, as you talked about, the “no-spy agreement” - how does this compare, perhaps, to the Five Eyes? And then I think: Is there something in the middle? Which is, in part, what I was trying to advocate in that paper.

The first point I’d like to make is: What is the status of PPD-28 in American law? And I think it could be misleading, a little bit, the title. It is a written directive from the president, binding the intelligence services as a matter of internal, executive branch law. There’s actually an Office of Legal Counsel opinion that says that directives like this - regardless of whether they are called Executive Orders or Policy Directives or anything else - do actually bind the departments and agencies. What they cannot do is bind anyone outside the government; that requires an act of the legislature, a statute. And it is true that a future president could change those, just like a future president could change an executive order. But PPD-28 will survive the next president in January. It won’t just go away. Those protections will continue to apply to employees of the NSA and all the other intelligence agencies.

Deutsche Übersetzung

Sachverständiger Timothy H. Edgar: *Herzlichen Dank, Herr Flisek. Ich denke, wir beginnen am besten mit der Frage nach dem Grundschutz, den die Presidential Policy Directive 28 allen Bürgern bietet. Und dann sollten wir auch über das No-Spy-Abkommen nachdenken, über das Sie sprachen - wie verhält sich dies eventuell zu der Gruppe der sogenannten Five Eyes? Und dann ist die Frage meiner Meinung nach: Gibt es etwas dazwischen? Das gehört zu dem, was ich in dieser Stellungnahme vorzuschlagen versucht habe.*

Zunächst möchte ich dabei die Frage nach dem Rechtsstatus der PPD-28 in den USA aufwerfen. Denn ich denke, der Name könnte ein wenig irreführend wirken. Es handelt sich um eine schriftliche Weisung des Präsidenten, die für die Geheimdienste bindend im Rahmen der internen Gesetze der Exekutive ist. Und es gibt sogar ein Rechtsgutachten des Office of Legal Counsel, wonach solche Direktiven - ob sie nun Executive Order oder Policy Directive oder sonst wie heißen - für die Ministerien und Behörden tatsächlich bindend sind. Sie sind jedoch nicht bindend für Personen oder Institutionen außerhalb der Regierung. Hierzu wäre ein Gesetz vonnöten. Und es stimmt, dass ein zukünftiger Präsident dies ändern könnte, ebenso wie er oder sie eine Executive Order ändern kann. Aber die PPD-28 wird den nächsten Präsidenten oder die nächste Präsidentin überleben, der oder die im Januar ins Amt kommt. Sie wird nicht einfach verschwinden. Diese Schutzanordnungen werden weiterhin für die Mitarbeiter der NSA und aller anderen Nachrichtendienste gelten.

Nur zur dienstlichen Verwendung

Original

And here I would like to agree with Dr. Halperin that, in some ways - although it seems less important, perhaps, than a broad decision that human rights law and principles apply, which is a controversial question; the U.S. government takes this unpopular, controversial position that is does not, PPD-28 gives you more concrete rules that apply to what an NSA employee is actually doing. The U.S. government could announce tomorrow that we are obeying human rights principles of proportionality and then humans rights organizations could argue that the United States government is not. It wouldn't actually change anything that the NSA does. Whereas PPD-28 does provide - although these are modest protections, I will admit - actual rules that, if you violate them, will be considered a violation of a binding obligation that you have to obey a directive of the president.

The question about political realism I think is an important one. There's a reason why Congress focused its attention on the bulk collection of American telephone records. Part of that was timing. The authority for that was going to expire last year, so they had to. But another part of it is: It was the big issue in the United States. These other issues we've been discussing today have been less important to the broad swath of the American public. But they were important enough to produce the reforms we've described - including PPD-28 - and part of that is because of the power of technology companies in the United States.

The industry in the United States was looking at a real problem with their global market: The perception as well as the reality of cooperating with the NSA gave foreign competitors a way in to an industry that has been until now - and still is - largely dominated by American companies. And

Deutsche Übersetzung

Und hier stimme ich Dr. Halperin insofern zu, als die PPD-28 auf gewisse Weise - auch wenn diese weniger bedeutend erscheinen mag als eine grundsätzliche Entscheidung, dass hier die Menschenrechtsgesetze und -grundsätze anzuwenden sind, was eine strittige Frage ist, denn die US-Regierung vertritt die wenig populäre und umstrittene Position, dass sie es nicht sind - konkretere Richtlinien für die tatsächliche Arbeit von Mitarbeitern der NSA bietet. Die Regierung der USA könnte morgen schon bekannt geben, dass wir die Menschenrechte und den Verhältnismäßigkeitsgrundsatz befolgen, und dann könnten Menschenrechtsorganisationen widersprechen und sagen, dass die US-Regierung dies nicht tut. An den tatsächlichen Aktivitäten der NSA würde das nichts ändern. Die PPD-28 dagegen bietet - und ich gebe zu, dass dies nur ein bescheidener Schutz ist - tatsächliche Regeln, wobei ein Verstoß gegen sie als Verstoß gegen die bindende Verpflichtung betrachtet würde, die Weisung des Präsidenten zu befolgen.

Die Frage nach dem politischen Realismus ist meiner Meinung nach wichtig. Der Kongress hat sich nicht ohne Grund mit der massenhaften Erfassung amerikanischer Telefondaten befasst. Teilweise war dies zeitbedingt. Die Frist hierfür wäre im vergangenen Jahr ausgelaufen, also mussten sie handeln. Ein weiterer Grund war aber die Tatsache, dass dies ein sehr wichtiges Thema in den Vereinigten Staaten war. Die anderen Themen, mit denen wir uns heute beschäftigt haben, waren der breiten Öffentlichkeit in den USA weniger wichtig. Sie waren jedoch wichtig genug, um zu den Reformen zu führen, die wir beschrieben haben, darunter auch die PPD-28. Und das liegt zum Teil an der Macht der Technologieunternehmen in den USA.

Die Technologiebranche in den USA sah sich mit einem echten Problem mit ihrem globalen Markt konfrontiert: Die öffentliche Wahrnehmung ihrer Zusammenarbeit mit der NSA und die Tatsache, dass es tatsächlich eine Zusammenarbeit gab, führten dazu, dass ausländische

Original

as President Obama and others in the government kept talking about the protections for United States persons and the U.S. person rules and privacy rules to protect Americans, many of these technology companies put pressure on the American government to say, This is not helping us globally to talk about protections for U.S. persons. If there are no protections for anyone else, then we can't make the argument that you should continue to use our services despite these revelations of involvement by the NSA.

And also foreign partners, including Germany, certainly put pressure on the Obama Administration. So I would say that those political realities are still there. And in the debate over Section 702 next year - over Prism and Upstream collection - we will have, I believe, an active involvement by companies as well as organizations who are looking to narrow or improve or reform those laws.

So my proposal, I guess, is a relatively modest one which is similar to Dr. Halperin's proposal, and that is to simply say, Between the broad swath of the entire world and what we can do to gather information from citizens of all countries, what privacy expectations people may have in their data and the very narrow club of Five Eyes partners that cooperate with each other and then largely do not collect and refrain from collecting intelligence on each other's soil, there may be a broader club that we could consider to be countries with strong democratic traditions, strong traditions of intelligence oversight, that we would agree should be limited in the use of their intelligence activities to specific types of purposes. And certainly international terrorism would be on that list, and then we could talk about what other kinds of security threats should be on that list.

Deutsche Übersetzung

Wettbewerber in einem Sektor Fuß fassen konnten, der bis dahin - und auch heute noch - weitgehend von US-Unternehmen dominiert wird. Und als dann Präsident Obama und andere Regierungsvertreter immer wieder über den Schutz amerikanischer Staatsbürger und über Personen- und Datenschutzvorschriften zum Schutz von Amerikanern sprachen, übten viele dieser IT-Unternehmen Druck auf die US-Regierung aus und sagten: Diese Erklärungen zum Schutz von US-Personen helfen uns auf globaler Ebene nicht weiter. Wenn alle anderen nicht auch geschützt werden, können wir ihnen nicht sagen, dass sie unsere Dienste trotz der Enthüllungen zu den Aktivitäten der NSA weiter nutzen sollen.

Und auch ausländische Partner, darunter auch Deutschland, setzten die Obama-Regierung unter Druck. Ich würde also sagen, dass diese politischen Realitäten nach wie vor Bestand haben. Und in die Debatte zu § 702 im kommenden Jahr - bezüglich Prism und der Upstream-Datenerfassung - werden sich meiner Meinung Unternehmen und Organisationen aktiv einmischen, die diese Gesetze gerne verschärfen bzw. verbessern oder reformieren möchten.

Mein Vorschlag ist daher wohl relativ bescheiden und ähnelt dem von Dr. Halperin. Es geht mir darum, dass es einen Mittelweg geben muss zwischen dem weltweit flächendeckenden Ansatz inklusive der Frage, was wir tun können, um Daten von Bürgern aller Nationen zu erfassen, und welche Erwartungen hinsichtlich des Datenschutzes diese Menschen haben, auf der einen Seite, und der sehr eng gefassten Gruppe der sogenannten Five Eyes, die zusammenarbeiten und weitgehend auf die Datenerfassung im Staatsgebiet der jeweils anderen verzichten, auf der anderen Seite. Dazwischen könnte es eine breitere Gruppe von Ländern geben, die wir als Staaten mit stabiler demokratischer Tradition betrachten, mit einer soliden Tradition von Kontrollsystemen über ihre Nachrichtendienste, und diese Länder könnten übereinkommen, die Nutzung ihrer nachrichtendienstlichen Aktivitäten auf bestimmte Zwecke zu beschränken.

Original

As to whether you would want to go further than that, maybe have an enlargement of the Five Eyes partners, I can tell you there would be a lot of resistance to that proposal inside the United States intelligence community establishment, really for a variety of reasons - probably historical, some having to do with language and culture. But perhaps Germany might have an argument for being included in that group if there's any interest in that. And that is that, of course, with the advent of Brexit and the British leaving the European Union, the United States has lost its closest partner inside the European Union which is also a member of the Five Eyes. And so I could imagine there's being an argument that having Germany as part of that group and making it into the Six Eyes instead of the Five Eyes, would then give the United States an advantage of having one of our close partners inside the European Union which we will lose when Britain leaves. That may not be a terribly convincing argument to the American national security establishment, but it seems to me to be a possible argument.

Realistically, though, I think it's more likely to think of a broader group of democratic countries that would agree to refrain from the broadest type of political spying in an enforceable way that involves using their institutions - in the United States that would be the Foreign Intelligence Surveillance Court; perhaps in Germany it would be something like the G 10 Commission, or this committee, or another committee, that would look broadly at external spying as well as at the internal spying that we have already regulated.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Deutschland ist natürlich auch

Deutsche Übersetzung

Einer dieser Zwecke wäre sicherlich die Bekämpfung des internationalen Terrorismus, und dann könnte man weiter darüber sprechen, welche anderen Arten von Sicherheitsrisiken dazu zählen sollten.

Was die Frage betrifft, ob man darüber hinausgeht und vielleicht die Gruppe der Five Eyes erweitert, so kann ich Ihnen sagen, dass dieser Vorschlag innerhalb der US-Geheimdienstkreise auf starken Widerstand treffen dürfte, aus verschiedenen Gründen, manche davon wahrscheinlich historisch, andere sprachlich und kulturell bedingt. Aber vielleicht spricht einiges dafür, Deutschland in diese Gruppe aufzunehmen, falls daran Interesse besteht, und zwar weil die USA mit dem Brexit-Beschluss und dem Austritt Großbritanniens aus der Europäischen Union ihren engsten Partner innerhalb der EU verloren haben, der auch Mitglied der Five Eyes ist. Ich kann mir daher vorstellen, dass darüber nachgedacht wird, Deutschland in diese Gruppe aufzunehmen und sie von Five Eyes auf Six Eyes zu erweitern, wodurch die Vereinigten Staaten den Vorteil gewännen, auch dann noch einen engen Partner innerhalb der EU in der Gruppe zu haben, wenn Großbritannien aus der EU austritt. Für die US-Geheimdienstkreise mag dies kein unbedingt überzeugendes Argument sein; aber es erscheint mir zumindest ein mögliches.

Für realistischer halte ich es jedoch, über eine breitere Gruppe demokratischer Länder nachzudenken, die übereinkommen, auf gegenseitige politische Spionage im weitesten Sinne zu verzichten, und zwar auf eine vollstreckbare Art und Weise unter Einbeziehung der entsprechenden Institutionen. In den USA wäre das der Foreign Intelligence Surveillance Court, in Deutschland vielleicht so etwas wie die G 10-Kommission oder dieser Ausschuss oder ein anderer Ausschuss, der die Auslandsspionage sowie die bereits gesetzlich geregelte Inlandsspionage kontrolliert.

Original

ein guter Partner, insbesondere im kritischen, aber darum vielleicht umso mehr fruchtbaren Dialog. - War da direkt eine Nachfrage? Sonst hätte ich jetzt Frau Gorski für die Beantwortung der zweiten Frage das Wort gegeben.

Christian Flisek (SPD): Vielleicht noch eben der Aspekt No-Spy-Abkommen, ob Ihnen so was in der Vergangenheit bekannt ist, dass die USA ein solches Agreement, einen solchen Vertrag mit irgendeinem anderen Staat haben.

Sachverständiger Timothy H. Edgar: The answer is essentially no, except that, of course, the other partners that the NSA has, which are called "third parties", around the world - - We have arrangements, bilateral arrangements with all of those parties that include whatever commitments those contain. So, the answer is, we do have those relationships. And part of the obligations, I think, of this committee has been to examine critically that relationship with the German BND, and to say, Has it respected the rights of Germans, has it respected the interests of Germany?

And so I think that in all of the relationships the NSA has around the world, because of the greater transparency there will continue to be more pressure from these other countries to ask, Are we doing enough to protect the privacy of our citizens? And so, any country that has that kind of close relationship with the United States, even beyond the Five Eyes, even if it's not a fully "no-spy agreement", does have some leverage to use to insist on greater protections than perhaps exist right now.

Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank. - Jetzt zur zweiten Frage Ashley Gorski, wenn ich das richtig erinnere.

Sachverständiger Dr. Morton H. Halperin: Could I make a comment on the first point before?

Deutsche Übersetzung

Sachverständiger Timothy H. Edgar: *Die Antwort lautet im Wesentlichen nein, wobei natürlich die anderen Partner der NSA weltweit, die sogenannten „dritten Parteien" - - Wir haben Absprachen, bilaterale Absprachen mit all diesen Parteien, in denen auch die entsprechenden Verpflichtungen enthalten sind. Die Antwort ist also, dass es solche Beziehungen gibt. Und zu den Aufgaben dieses Ausschusses hier zählt meines Wissens auch, die Beziehung zum deutschen BND kritisch zu untersuchen und zu klären, ob der BND die Rechte der Deutschen und die Interessen Deutschlands respektiert hat.*

Und ich denke, dass die größere Transparenz dazu führen wird, dass in all diesen weltweiten Beziehungen der NSA mehr Druck von den anderen Staaten kommen wird, wenn es um die Frage geht, ob sie genug tun, um die Privatsphäre ihrer Bürger zu schützen. Also hat jedes Land, das diese Art der engen Beziehungen zu den Vereinigten Staaten pflegt, auch über die Gruppe der Five Eyes hinaus, auch ohne umfassendes No-Spy-Abkommen ein gewisses Maß an Einfluss und kann auf stärkeren Schutz bestehen, als es zurzeit vielleicht gibt.

Sachverständiger Dr. Morton H. Halperin: *Könnte ich kurz etwas zu dem zuvor Gesagten sagen?*

Original

Vorsitzender Dr. Patrick Sensburg: Normally, no. Sorry. It would bring it a little bit in disorder. Sorry for that. - Ashley Gorski.

Sachverständige Ashley Gorski: And so if I understand your question, you are interested in how I or one would go about assessing cooperation between the NSA and the BND outside of official channels from 2001 to the time of the Snowden disclosures in 2013. And here I think I would begin with the reporting that came out of the Snowden disclosures that's incredibly far-reaching and covers not only programs and information-sharing that was happening at the time of the Snowden disclosures but covers programs and information-sharing and relationships between countries that predate those disclosures and go much farther back. And, in my written testimony, I discuss more than a dozen programs that have been disclosed by Snowden but also by the reporters who've done a tremendous amount of legwork to place those programs in context and also speak about information-sharing. So, I would begin there.

If, after surveying the landscape there, you're still looking for more information, I think it would be essential to understand the scope of the NSA's surveillance in order to get a handle on what may or may not have been shared with the BND. And so there I would look to the surveillance authorities themselves. And in that time period EO 12333 was still in effect. Mass surveillance and bulk surveillance abroad are still happening.

And I would also look to the historical technological landscape. As my colleague Dr. Soghoian mentioned earlier, in a pre-Snowden era, email was not typically encrypted by the - - I guess Google did it in 2010. But in this era starting in

Deutsche Übersetzung

Vorsitzender Dr. Patrick Sensburg: *Normalerweise nicht, nein. Ich bedaure. Das würde die Reihenfolge etwas durcheinander bringen. Es tut mir leid. - Ashley Gorski.*

Sachverständige Ashley Gorski: *Wenn ich Ihre Frage richtig verstehe, möchten Sie gerne wissen, wie ich oder wie man überhaupt an die Einschätzung der Zusammenarbeit von NSA und BND außerhalb der offiziellen Kanäle im Zeitraum zwischen 2001 und den Snowden-Enthüllungen 2013 herangehen würde. Und ich denke, ich würde mit der unglaublich weitreichenden Berichterstattung beginnen, die sich aus den Snowden-Enthüllungen ergab und die nicht nur die Programme und Informationsweitergabe zum Zeitpunkt der Enthüllungen betrifft, sondern auch Programme und Informationsweitergaben und Beziehungen zu anderen Ländern, die zeitlich weiter zurückgehen. In meiner schriftlichen Stellungnahme erörtere ich über ein Dutzend Programme, die durch Snowden, aber auch durch die Journalisten aufgedeckt wurden, die einen sehr großen Rechercheaufwand geleistet haben, um diese Programme in einen Gesamtzusammenhang zu stellen, und ich spreche darin auch über die Informationsweitergabe. Damit würde ich also anfangen.*

Wenn Sie nach der Betrachtung dieser Landschaft noch weitere Informationen suchen, dann ist es, so denke ich, wesentlich, das Ausmaß der Überwachung durch die NSA zu verstehen, um einen Ansatzpunkt dafür zu bekommen, was möglicherweise an den BND weitergegeben wurde und was nicht. Und hier würde ich mir die Überwachungsbehörden selbst ansehen. Und in diesem Zeitraum war EO 12333 noch in Kraft. Es wurden weiterhin Massenüberwachungen und die massenhafte Erfassung und Auswertung von Daten im Ausland durchgeführt.

Außerdem würde ich mir die damalige Technologielandschaft ansehen. Wie mein Kollege Dr. Soghoian vorhin sagte, wurden E-Mails vor den Snowden-Enthüllungen normalerweise nicht standardmäßig verschlüsselt. Ich glaube, Google

Original

2001, the NSA had different incentives to do things as we know that are done, like hack into Google's and Yahoo's data centers abroad, or hack into the traffic that was transiting between those data centers, because so much email was unencrypted. So that's another factor I would take into account.

And then, finally, I would also think about U.S. domestic executive branch understandings of the surveillance authorities out of hand. In this era, you had what's known as the "President's Surveillance Program", parts which are referred to as "stellar wind" in which the Bush administration, relying on an extraordinary view of its own executive authority and believing that it could override a duly enacted law - the Foreign Intelligence Surveillance Act - engaged in a sweeping warrantless surveillance program. And, due to Freedom of Information Act requests, and again reporting, we've learned a great deal about the surveillance that was taking place during this period. So that's where I would begin.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich habe jetzt auf der Rednerliste Kollegen von Notz, Kollegen Wendt, dann mich noch mal, dann den Kollegen Ströbele. Dann habe ich Herrn Hahn, dann Frau Warken. - Dann ist Kollege von Notz jetzt dran.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. - Vielen Dank an die Sachverständigen. Ich möchte Ihnen auch noch mal persönlich danken, einmal dafür, dass Sie den weiten Weg auf sich genommen haben und zu uns gekommen sind, und auch für Ihr hohes Engagement in den letzten Jahre in diesen zivilgesellschaftlichen, für uns sehr relevanten Fragen. Wenn ich Ihren Ausführungen zugehört habe, kann ich Ihnen

Deutsche Übersetzung

hat das 2010 getan. Aber in diesem Zeitraum ab 2001 hatte die NSA andere Motive, die Dinge zu tun, von denen wir wissen, dass sie getan wurden, beispielsweise sich in die ausländischen Datenzentren von Google und Yahoo einzuhacken oder in den Datenverkehr zwischen diesen Datenzentren, denn die meisten E-Mails waren damals unverschlüsselt. Das ist also ein weiterer Gesichtspunkt, den ich berücksichtigen würde.

Und schließlich würde ich mich damit beschäftigen, welches Verständnis die Exekutive in den USA von den bestehenden Überwachungsbehörden hatte. In jener Zeit gab es das, was als „President's Surveillance Program" und in Teilen als „Stellar Wind" bekannt ist. Mit diesem Programm führte die Bush-Regierung ein flächendeckendes und unbegründetes Überwachungsprogramm durch, ausgehend von einer erstaunlichen Auffassung ihrer eigenen exekutiven Befugnis und dem Glauben, dass sie sich damit über ein ordnungsgemäß verabschiedetes Gesetz - den Foreign Intelligence Surveillance Act - hinwegsetzen könne. Aufgrund von Anfragen im Rahmen des Freedom of Information Act und auch hier wieder aufgrund von journalistischer Recherche wissen wir sehr viel über die Überwachung, die in diesem Zeitraum stattgefunden hat. An diesen Punkten würde ich also ansetzen.

Original

sagen, dass die Diskussionen, die wir mit unseren Diensten führen, auch zur Notwendigkeit von parlamentarischer Kontrolle und rechtstaatlichen Grundsätzen, sehr, sehr ähnlich sind wie die Diskussion, die Sie führen.

Ich habe eine ganze Reihe von Fragen. Ich will aber zwei Fragen an den Anfang stellen. Vielleicht in Bezug auf das Eingangsstatement noch mal an Mrs. Gorski die Frage, ob es nach Ihrer Einschätzung und Ihren Interpretationen der Snowden-Veröffentlichungen zu massenhafter Überwachung oder Analyse von deutschen Kommunikationsverkehren durch die NSA gekommen ist.

Die zweite Frage richtet sich an Herrn Soghoian im Hinblick auf die technische Überlegung, weil wir jetzt ganz viel davon gehört haben auch im Hinblick auf die Reformdiskussion in den USA „Wie ist das mit US-Citizens und Non-US-Citizens?“: Inwieweit kann man überhaupt bei „bulk data“ ebendiese Nationalität in der Analyse klären? Es ist ja nicht so, dass auf jedem Datum eine kleine Flagge ist, welche Nationalität dieser Kommunikationsverkehr oder das „data“ eben hat. Und deswegen die Frage: Wie zuverlässig kann ich überhaupt feststellen, wenn ich Daten anfasse, mit welcher Nationalität von Daten ich es zu tun habe? Und wenn Sie keine Prozentzahl sagen können, vielleicht können Sie einen Eindruck vermitteln, wie das überhaupt geschieht, weil wir sehr viel über Filter diskutiert haben hier die letzten Jahre, auch im Hinblick, inwieweit man solche Sachen zuverlässig filtern kann oder eben erst, wenn man Sachen anschaut, also im Vorfeld filtern kann, bevor man ein Datum oder Daten sich anschaut, oder ob man dann erst darauf kommen kann, wenn man sich die Sachen tatsächlich anguckt, oder vielleicht auch selbst dann häufig bei anderen Dingen als Telefonnummern oder E-Mail-Verkehren einfach große Probleme hat mit der nationalen Zuordnung von Daten. - Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Wir würden mit Frau Gorski beginnen, wenn das okay ist.

Deutsche Übersetzung

Nur zur dienstlichen Verwendung

Original

Sachverständige Ashley Gorski: So, in the summer of 2013, *Der Spiegel* reported that the NSA was collecting and retaining data from approximately 500 million German phone and Internet communications each month. Whether that degree of data collection is ongoing, I can't say, but that is the reporting as of that time. I would certainly characterize that as mass surveillance. Whether the U.S. government would characterize that as bulk surveillance is a different question. As discussed earlier, bulk surveillance is a term of art. To acquire these 500 million communications, it is possible that selectors of a sort, or discriminants of a sort, were used, in which case the government may contend that it's not bulk surveillance. But I think that certainly qualifies as bulk or mass surveillance.

Sachverständiger Dr. Christopher Soghoian: So with regards to your question: One of the most interesting disclosures to date was a publication by Glenn Greenwald of two documents: the NSA's targeting procedures and the NSA's data retention procedures. Both of these were published, I think, in 2013. And they really reveal the extent to which the NSA both seeks to identify and differentiate between the foreign, non-U.S., and U.S. communications. As you hinted, it's somewhat easy for telephone numbers. If the U.S. government is monitoring communication, and it sees a number with +1 - the U.S. and Canadian country code -, then it can reasonably assume that that's a U.S. communication. Things get a little bit more complicated for email, and then even more complicated for data on the Web.

From those targeting procedure documents, we see some interesting things. So, for example, one of the things the NSA does is it works with U.S. telecommunications carriers to obtain, either in real time or in near real time, information revealing when foreign telephones land in the United States. So, for example, if you're a German citizen, you're being targeted by the NSA, and then

Deutsche Übersetzung

Sachverständige Ashley Gorski: *Im Sommer 2013 berichtete „Der Spiegel", dass die NSA jeden Monat Daten von etwa 500 Millionen Telefon- und Internetverbindungen in Deutschland erfasste und speicherte. Ob eine Datenerfassung in diesem Ausmaß immer noch stattfindet, kann ich nicht sagen; aber so lautete die damalige Berichterstattung. Ich würde das ganz gewiss als Massenüberwachung bezeichnen. Ob die US-Regierung es auch als Massenüberwachung bezeichnen würde, ist eine andere Frage. Möglicherweise wurde zur Erfassung dieser 500 Millionen Verbindungen irgendeine Form von Selektoren oder Diskriminanten verwendet, und in diesem Fall könnte die Regierung behaupten, dass es sich nicht um Massenüberwachung handelt. Doch in meinen Augen entspricht das durchaus einer Massenüberwachung.*

Sachverständiger Dr. Christopher Soghoian: *Bezugnehmend auf Ihre Frage - zu den bisher interessantesten Enthüllungen zählte die Veröffentlichung zweier Dokumente durch Glenn Greenwald: zum Targeting-Verfahren der NSA und zu ihren Datenspeicherungsverfahren. Beide Dokumente wurden, so glaube ich, 2013 veröffentlicht. Und sie zeigen wirklich auf, in welchem Ausmaß die NSA ausländische, Nicht-US-Verbindungen zu erkennen und zwischen ihnen und US-Verbindungen zu differenzieren versucht. Wie Sie andeuteten, ist das bei Telefonnummern relativ einfach. Wenn die US-Regierung die Telefonkommunikation überwacht und eine Nummer mit dem Ländercode +1 für die USA und Kanada sieht, kann sie vernünftigerweise davon ausgehen, dass es sich um eine US-Verbindung handelt. Bei E-Mail wird die Sache schon etwas komplizierter, und mehr noch beim Datenverkehr im Internet.*

Aus den Dokumenten zum Targeting-Verfahren können wir Interessantes ersehen. So besteht zum Beispiel ein Vorgehen der NSA darin, mit US-amerikanischen Telekommunikationsunternehmen zusammenzuarbeiten, um in Echtzeit oder beinahe Echtzeit informiert zu werden, wenn Mobiltelefone aus dem Ausland in den Vereinigten Staaten ankommen. Wenn Sie also

Original

you get on an airplane and you fly from Berlin to New York, the moment you land in New York and you turn your phone on, your phone will register with a U.S. telecommunications carrier - you're now roaming - that will alert the NSA and they will say, "Oh, hang on. Now this person is a U.S. person under U.S. law and we actually have to give them more protections than if we were spying on them back in Germany." I suspect that the NSA is not the only intelligence service that is monitoring the arrival of foreign telephones to its country, and I suspect that many intelligence services, including the Germans, are probably also monitoring which of its citizens are going abroad. So, for example, if you had a scenario where a German citizen is suddenly starting roaming in Syria, I imagine that your own intelligence services would probably be paying close attention to that. And that might be something that you should look into.

I think the most interesting part of your question, though, is not: What happens when the NSA identifies a foreign user's data or a U.S. person's data? The most interesting question is: What happens when they cannot identify the country of origin? And I think that brings us to the sort of perverse situation we have right now, which is: What happens when someone uses a technology like Tor or VPN that hides your location? If you're a U.S. person and you send your data to Europe using Tor, you may lower your privacy protection under the law. And if, for example, the U.S. has decided to give the Germans some elevated level of protection but it has not given that same level of protection to people in India, and then Germans send communications through India, now are they lowering their protections?

We know, again, from the NSA targeting document that when the NSA cannot determine the

Deutsche Übersetzung

beispielsweise als Deutscher von der NSA überwacht werden und mit dem Flugzeug von Berlin nach New York fliegen, dann meldet sich Ihr Mobiltelefon in dem Moment, in dem Sie es nach der Landung in New York einschalten, bei einem US-amerikanischen Telekommunikationsanbieter an. Sie nutzen nun das amerikanische Netz, und der Anbieter verständigt die NSA, und die sagen: Moment! Diese Person gilt jetzt als US-Person und untersteht dem Gesetz der USA und damit tatsächlich stärkerem Schutz, als wenn wir sie zuhause in Deutschland ausspionieren. - Ich nehme an, dass die NSA nicht der einzige Nachrichtendienst ist, der überwacht, ob ausländische Mobiltelefone in seinem Land eintreffen, und ich nehme an, dass viele Nachrichtendienste, auch die deutschen, ebenfalls überwachen, welche ihrer Bürger ins Ausland reisen. Wenn man also beispielsweise ein Szenario nimmt, in dem ein deutscher Staatsbürger plötzlich anfängt, mit seinem Mobiltelefon ein syrisches Telefonnetz zu nutzen, dann kann ich mir vorstellen, dass Ihre eigenen Nachrichtendienste das aufmerksam beobachten würden. Und das ist etwas, dem Sie nachgehen sollten.

Ich denke jedoch, dass der interessanteste Teil Ihrer Frage nicht ist, was passiert, wenn die NSA die Daten eines ausländischen Nutzers oder einer US-Person identifiziert. Interessanter ist die Frage, was passiert, wenn sie das Ursprungsland nicht identifizieren kann. Und das führt uns zu der etwas verrückten Situation, in der wir uns jetzt befinden, nämlich: Was geschieht, wenn jemand eine Technologie wie Tor oder VPN nutzt, die den Standort verschleiern? Wenn eine US-Person über Tor Daten nach Europa sendet, schwächt sie damit möglicherweise den gesetzlichen Schutz ihrer Privatsphäre. Und wenn die USA beispielsweise beschließen, Deutschen ein höheres Maß an Schutz zu bieten, den Menschen in Indien jedoch nicht, schwächen die Deutschen dann ihren Schutzgrad, wenn sie Verbindungen über Indien schicken?

Aus dem Targeting-Dokument der NSA wissen wir auch, dass die NSA Verbindungen, deren

Original

origin, the communications are treated as a foreigner's communications and get the lowest protection under the law. You're right: There are no flags that are attached to communications content, and in fact technologies like Tor will strip off any flags that might be there; you don't want to identify these. Or you could also imagine a situation if attaching a U.S. flag to a communication gave it higher protections, then everyone that was being targeted by the NSA would attach a U.S. flag to avoid the surveillance.

You know, it troubles me that I might receive lower protections under the law, under my country's laws, by employing privacy technologies to try and protect my communications. I don't think that individuals should have to pick between technical protections or legal protections. But as long as the NSA treats unknown communications as foreign, even U.S. persons may be taking risks by sort of laundering their data through foreign countries.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank auch für diese Ausführungen. - Wir kommen jetzt zu den Fragen vom Kollegen Wendt.

Marian Wendt (CDU/CSU): Vielen Dank. - Guten Tag! Edward Snowden hat ja Behauptungen aufgestellt, die dahin gehen, dass verschiedene US-Unternehmen Informationen und persönliche Daten an die Nachrichtendienste der USA liefern müssen. Als diese Vorwürfe in den öffentlichen Raum kamen vor einigen Jahren: Vielleicht könnten Sie, Herr Edgar, mal beschreiben, wie die öffentliche Stimmung in den USA war. Gab es da einen großen Aufschrei? Gab es da negative Presse? Gab es da Kampagnen? Gab es da Forschung? Oder war so eher die Stimmung: „Na ja, gut, es dient unserer nationalen Sicherheit; ist okay, wenn das gemacht wird, und ich möchte

Deutsche Übersetzung

Ursprung sie nicht ermitteln kann, als ausländische Verbindungen behandelt, die den schwächsten gesetzlichen Schutz genießen. Sie haben ganz recht: Kommunikationsinhalte sind nicht durch Flaggen gekennzeichnet, und Technologien wie Tor entfernen sogar alle Flaggen, die es vielleicht geben mag, denn man will den Nutzer nicht identifizieren. Vorstellbar ist auch, dass in dem Fall, dass die Kennzeichnung von Verbindungen mit einer US-Flagge den Schutzgrad erhöht, alle, die von der NSA überwacht werden, diese Kennzeichnung durch eine US-Flagge nutzen würden, um der Überwachung zu entgehen.

Wissen Sie, es stört mich, dass ich möglicherweise ein geringeres Maß an Schutz durch das Gesetz meines Landes genieße, wenn ich meine Kommunikationsinhalte durch Datenschutztechnologien zu schützen versuche. Ich finde nicht, dass Menschen vor die Wahl zwischen technischem Schutz oder rechtlichem Schutz gestellt werden sollten. Doch solange die NSA Verbindungen unbekannten Ursprungs als ausländische Verbindungen behandelt, gehen auch US-Personen Risiken ein, wenn sie ihre Daten sozusagen über das Ausland „waschen“.

Original

ja wissen, wenn Terroristen über Facebook miteinander kommunizieren; dann sollten das auch die Nachrichtendienste wissen, und deswegen ist es so okay“? Also, vielleicht könnten Sie diese Stimmung beschreiben, als erste Frage.

Und die zweite Frage ist: Wird bei US-Unternehmen, die in Europa agieren, die ja auch europäischen Rechten unterstellt sind, entsprechend gewährleistet, dass die Daten von EU-Bürgern bzw. Ausländern oder auch US-Amerikanern, die hier die Dienste nutzen, ordentlich geschützt werden? Und wie beurteilen Sie in diesem Zusammenhang vor allen Dingen Privacy Shield? Weil ja in Europa gespeicherte Daten anderes Recht sind, als wenn sie zum Beispiel in den USA gespeichert werden, und es da ja auch unsererseits gewisse verschiedene Vorstellungen gibt, wie mit diesen Daten umzugehen ist. Und das sollte entsprechend mit dem Privacy Shield ja auch geregelt werden. - Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: Auch an Herrn Edgar?

Marian Wendt (CDU/CSU): Ja.

Vorsitzender Dr. Patrick Sensburg: Ja. Okay. - Herr Edgar.

Sachverständiger Timothy H. Edgar: Thank you, Mr. Wendt. - So, on the first question: It really was not a revelation of Edward Snowden that U.S. companies had to provide this information, but he did provide more details as to how this worked. And that’s why there was actually a significant reaction, I would say, of the American public, but more of the tech community and the tech companies themselves. And this has to do with both the Prism and Upstream collection programs that we’ve been discussing.

So both of those programs are conducted under Section 702 of the Foreign Intelligence Surveillance Act, which was added by the FISA

Deutsche Übersetzung

Sachverständiger Timothy H. Edgar: *Vielen Dank, Herr Wendt. Zur ersten Frage: Dass die US-Unternehmen diese Informationen zur Verfügung stellen mussten, wurde nicht erst durch Edward Snowden enthüllt; allerdings hat er genauere Einzelheiten dazu vorgelegt, wie dabei vorgegangen wurde. Und darum gab es eine deutliche Reaktion, so würde ich sagen, seitens der amerikanischen Öffentlichkeit, mehr jedoch seitens der Technologiebranche und der IT-Unternehmen selbst. Und dies hat sowohl mit dem Prism-Programm zu tun als auch mit der Upstream-Datenerfassung, über die wir gesprochen haben.*

Beide Programme wurden nach § 702 des Foreign Intelligence Surveillance Act durchge-

Original

Amendments Act of 2008. So it was not actually a secret that the government could demand this information, but the details of how it did so and the fact that it was requesting or demanding, I should say, data from U.S. tech companies and from the Internet backbone was not known; that was classified. But the existence of the authority was not.

And referring back to the summer of 2008, where President Obama came and gave this speech in Germany. There was another important event, which was a debate within the Obama campaign, about whether Senator Obama should vote for that law. And he decided to vote in favor of Section 702 of FISA, the FISA Amendments Act. It was one of the most controversial decisions he took, within his own activists. So sometimes we forget that President Obama did not necessarily change his opinion on some of these issues; he had already voted for that program Section 702 of FISA.

So I would say, just to sum up, the atmosphere was surprise at just how this law does work in practice, but the existence of that authority and some of the debates about it had already happened in the summer of 2008. But that had happened at a more abstract level. And obviously it makes a big difference when you hear about the abstract ability of the NSA to go and get an order by the FISA Court to get data that might happen to be in the United States, and the actual way in which the program is working and how many selectors are being used under Prism, exactly how we scan traffic from the Internet backbone.

Deutsche Übersetzung

führt, ein Abschnitt, der mit dem Änderungsgesetz zum Foreign Intelligence Surveillance Act 2008 in Kraft trat. Es war also kein Geheimnis, dass die Regierung diese Informationen einfordern konnte; doch die genaueren Einzelheiten zum Vorgehen waren nicht bekannt, ebenso wenig wie die Tatsache, dass die Regierung Daten von IT-Unternehmen und vom Internet-Backbone abfragte bzw. eher einforderte. Das war Verschlusssache, nicht jedoch die Tatsache, dass die Regierung diese Befugnisse hatte.

Und um noch einmal zum Sommer 2008 zurückzukommen, als Präsident Obama auf Deutschlandbesuch kam und hier seine Rede hielt: Es gab damals noch ein weiteres wichtiges Ereignis, nämlich die Diskussion innerhalb des Obama-Lagers, ob Senator Obama für das Gesetz stimmen solle. Und er entschied sich, für § 702 des FISA, den FISA Amendments Act [Änderungsgesetz zum Gesetz zur Überwachung in der Auslandsaufklärung] zu stimmen. Dies zählte zu den unter seinen Anhängern am meisten umstrittenen Entscheidungen. Wir vergessen also manchmal, dass Präsident Obama seine Haltung zu diesen Fragen nicht zwangsläufig geändert hat; denn er hat bereits mit seiner Stimme für § 702 des FISA für dieses Programm gestimmt.

Zusammenfassend würde ich also sagen, dass man überrascht war, wie genau dieses Gesetz in der Praxis angewendet wurde. Doch die Tatsache, dass es diese Befugnisse gab, war bekannt, und die Debatten darüber hatten bereits im Sommer 2008 stattgefunden. Doch das geschah auf einer eher abstrakten Ebene. Und natürlich ist es ein großer Unterschied, ob man von der abstrakten Möglichkeit hört, dass die NSA einen Beschluss vom Foreign Intelligence Surveillance Court einholen kann, um an Daten zu kommen, die vielleicht in den Vereinigten Staaten gespeichert sind, oder ob man sieht, wie dieses Programm in der Realität funktioniert und wie viele Selektoren mit Prism eingesetzt werden und auf welche Weise genau wir den Datenverkehr am Internet-Backbone überwachen.

Original

On the issue of Privacy Shield, I guess I go back and forth on this. I was not terribly impressed with any of the substance of the guarantees that the U.S. government made in the Privacy Shield to Europeans to satisfy the Schrems decision. The bottom line is, I do not think the Privacy Shield does satisfy the Schrems decision. With that said, two things that I think are positive from that: One is, they did create an ombudsman for European citizens to complain to in the State Department. So that goes back to a question of Ms. Renner's. You know, how effective that mechanism is going to be we will see in practice. But if you want to complain as a European citizen, you do have an avenue of complaining to the ombudsperson in the State Department. Then there will be a process inside the government for somehow resolving that complaint. The second point is that it forced the intelligence community - - And, in fact, Robert Litt, the General Counsel of the Office of the Director of National Intelligence, who I've worked with for years actually, wrote an extensive letter that basically said, Here are all the protections, safeguards and oversight that we apply to our intelligence agencies, including PPD-28 and some of the things we have done since the Snowden reforms.

And although that in and of itself doesn't change anything - and like I said, I don't think it's good enough to satisfy Schrems - I do think it was an important exercise. Because it essentially laid down a marker that says that if you're going to challenge our use of data by our intelligence services, we can't simply say, This is national security, so go away. - We do actually have to lay out what is our system.

And one question that I think needs to be answered by European countries, including Germany, is: So does this mean European countries

Deutsche Übersetzung

Was den EU-US Privacy Shield angeht, so bin ich unschlüssig. Ich war nicht sonderlich beeindruckt vom Inhalt der Zusicherungen, die die US-Regierung den Europäern im Privacy Shield macht, um die Vorgaben des Schrems-Urteils zu erfüllen. Unterm Strich denke ich nicht, dass die Vorgaben des Schrems-Urteils durch den EU-US Privacy Shield erfüllt sind. Dennoch gibt es dabei meiner Meinung nach zwei positive Aspekte. Erstens wurde im State Department eine Ombudsstelle geschaffen, an die EU-Bürger sich mit Beschwerden wenden können. Das also zu einer der Fragen von Frau Renner. Wissen Sie, wie wirksam dieser Mechanismus ist, wird sich in der Praxis zeigen. Aber wenn Sie als EU-Bürgerin eine Beschwerde vorbringen möchten, gibt es einen Beschwerdeweg über die Ombudsstelle im State Department. Es gibt dann ein Verfahren innerhalb der Regierungsbehörden, um die Beschwerde zu klären. Der zweite positive Aspekt ist, dass die Nachrichtendienste gezwungen wurden - - Und Robert Litt, General Counsel des Office of the Director of National Intelligence, mit dem ich mehrere Jahre zusammengearbeitet habe, hat einen ausführlichen Brief geschrieben, in dem er im Grunde sagte: Hier sind sämtliche Schutzvorkehrungen, Absicherungen und Kontrollmaßnahmen, die wir auf unsere Nachrichtendienste anwenden, darunter auch die PPD-28 und einige der Dinge, die wir seit den Snowden-Reformen eingeführt haben.

Und auch wenn sich dadurch allein nichts geändert hat - und, wie gesagt, ich denke nicht, dass es ausreicht, um die Vorgaben des Schrems-Urteils zu erfüllen -, so denke ich doch, dass es ein wichtiger Schritt war. Denn es wurde damit im Grunde ein Zeichen gesetzt, dass wir, wenn jemand die Nutzung von Daten durch unsere Nachrichtendienste infrage stellt, ihn nicht einfach mit der Behauptung abschmettern können, dass es sich um eine Frage der nationalen Sicherheit handelt. Sondern wir müssen tatsächlich offenlegen, was unser System ist.

Und eine Frage, die meiner Meinung nach die europäischen Länder beantworten müssen, darunter auch Deutschland, ist diese: Bedeutet

Original

should also have to write a Bob-Litt-style letter about what the protections are that their agencies afford to data that is stored in their jurisdictions? And if you look at a report by, I think, the EU Fundamental Rights Agency, there aren't very many protections. Certainly, I would say, my own estimation is that the United States is pretty much at the top of the heap when it comes to legal and policy protections. Germany and the U.K. are actually pretty good in comparison to some other countries around the world. But all of us, including the United States, could use some improvement. So I would say that there have been some, you might say, baby steps since 2013 - maybe even bigger steps in time - but that we still need to continue to have a conversation about this. We will be having a much bigger conversation next year about Section 702 of FISA, which comes up for renewal.

Vorsitzender Dr. Patrick Sensburg: Okay. Ganz herzlichen Dank. - Ich hätte zwei Fragen an Mrs. Gorski und an Mr. Soghoian. Es geht beide Male um Google, Yahoo, Facebook und andere.

Mrs. Gorski, Sie hatten gesagt, wenn ich es richtig verstanden habe, dass man auf 117 000 Accounts Zugriff hatte - wenn ich das Eingangsstatement richtig verstanden habe. Gibt es dafür Beweise, oder ist das, sagen wir mal, auch nur Zeitungswissen? Denn Sie hatten auf die Frage eben geantwortet, 500 Millionen Kommunikationen, das hätten Sie aus der Zeitung. Jetzt interessiert uns natürlich: Gibt es dafür irgendwelche Nachweise, haben Sie da was? Insbesondere wird ja Google, Yahoo, Facebook, Twitter der Vorwurf gemacht, aufgrund der Gesetzgebung teilweise verlängerter Arm der NSA zu sein. Was für Erkenntnisse haben Sie in letzter Zeit gewinnen können oder in der Vergangenheit gewinnen können, die das auch mit Fakten hinterlegen?

Fast die ähnliche Frage an Herrn Soghoian. Sie sagten, Twitter, Facebook, Google nehmen es

Deutsche Übersetzung

dies, dass auch die EU-Länder einen Brief in der Art von Bob Litt schreiben müssten, in dem sie darlegen, wie ihre Nachrichtendienste die Daten schützen, die in ihren Hoheitsgebieten gespeichert werden? Und wenn Sie sich den Bericht der, ich glaube es war die Agentur der Europäischen Union für Grundrechte ansehen, dann werden Sie feststellen, dass es nicht viele Schutzvorkehrungen gibt. Meiner Einschätzung zufolge sind die Vereinigten Staaten so ziemlich an der Spitze, was rechtliche und politische Schutzrichtlinien betrifft. Deutschland und Großbritannien stehen im Vergleich zu einigen anderen Ländern weltweit auch ziemlich gut da. Aber bei allen, auch den USA, besteht Verbesserungsbedarf. Ich würde also sagen, dass es seit 2013 einige, man könnte sagen, winzige Schritte gab und mit der Zeit vielleicht auch größere Schritte, aber dass es immer noch einen Bedarf an Gesprächen zu diesem Thema gibt. Eine sehr viel größere Debatte werden wir im kommenden Jahr führen, wenn die Verlängerung von § 702 des FISA ansteht.

Original

nicht so ernst mit dem Datenschutz - wenn ich es jetzt etwas zusammenfasse; ich hoffe, ich gebe Sie jetzt nicht falsch wieder. Ja, die Unternehmen standen ziemlich am Pranger nach den Veröffentlichungen 2013 und sind wieder aus dem Rampenlicht heraus. Hat sich was total geändert? Ist es die End-zu-End-Verschlüsselung von WhatsApp, die alles gut macht? Wie bewerten Sie die Lage?

Sachverständige Ashley Gorski: So, to begin, the figure: As of April 2013, the NSA was monitoring at least 117,000 targeted accounts via Prism. That is based on reporting in *The Washington Post*, but the reporting itself highlights NSA slides that contain that specific number and tie it specifically to Prism. And I would also note that separately the government itself has made more general disclosures about the number of Section 702 targets as a whole. And those numbers are in the tens of thousands. I think the most recent disclosure, if I'm remembering correctly, was more than 90,000. I don't recall if it exceeded 100,000.

Sachverständiger Timothy H. Edgar: 93,000.

Sachverständige Ashley Gorski: 93,000. So that is an official government disclosure, that there are 93,000 targets under Section 702.

Sachverständiger Dr. Christopher Soghoian: Let me try and clarify what's going on with the companies and their approach to security and surveillance. Prior to 2010, most technology companies were not employing any form of encryption, really, for their users' communications. What that meant was that intelligence agencies like the NSA, but not limited to just the NSA, could collect the communications of users without even going to Google.

Let me be clear: Given a choice between going to a national telephone company and going to a technology company, intelligence services will

Deutsche Übersetzung

Sachverständige Ashley Gorski: *Beginnen wir mit der Zahl: Mit Stand vom April 2013 überwachte die NSA über Prism mindestens 117 000 Zielkonten. Die Zahl basiert auf Berichten der „Washington Post", aber die Berichterstattung selbst gibt Präsentationsfolien der NSA wieder, auf denen die genaue Zahl genannt und direkt mit Prism in Verbindung gebracht wird. Außerdem weise ich darauf hin, dass die Regierung selbst allgemeinere Informationen zur Gesamtzahl der Zielkonten im Rahmen von § 702 offengelegt hat. Und diese Zahlen bewegen sich im fünfstelligen Bereich. Der jüngsten Auskunft zufolge waren es, wenn ich mich richtig erinnere, über 90 000. Ich weiß nicht, ob es über 100 000 waren.*

Sachverständiger Timothy H. Edgar: *93 000.*

Sachverständige Ashley Gorski: *93 000. Der offiziellen Auskunft der Regierung zufolge gibt es also 93 000 Zielkonten im Rahmen von § 702.*

Sachverständiger Dr. Christopher Soghoian: *Lassen Sie mich versuchen, zu verdeutlichen, wie es sich mit den Unternehmen und ihrer Herangehensweise an Sicherheit und Überwachung verhält. Vor 2010 nutzten die meisten Unternehmen keinerlei Form der Verschlüsselung für die Kommunikationsinhalte ihrer Nutzer. Das bedeutete, dass Nachrichtendienste wie die NSA, aber auch andere die Kommunikationen von Nutzern erfassen konnten, ohne sich auch nur an Google zu wenden.*

Lassen Sie mich das ganz deutlich sagen: Wenn Nachrichtendienste die Wahl haben, ob sie sich lieber an einen nationalen Telefonanbieter oder

Original

always go to a national telephone company. In many countries, the national telephone company used to be part of the government. They may have been part of the post office or another agency. They have a long, long, deep relationship with the intelligence apparatus, and they will bend over backwards to help governments. So, prior to 2010, a user's emails, a user's text messages, a user's social media information could be collected without going to Google, without going to Facebook and without going to Twitter. They could do it just by collecting in bulk Internet information and then looking through that for unencrypted communications and deciphering those.

Starting in 2010, a trend began in the U.S. tech industry towards using encryption to protect data from the customer to the technology company. And really Google has probably been the biggest pioneer in this space, but Twitter and Facebook have also been pretty good. Yahoo, really, was pretty atrocious until the Snowden disclosures, when they were finally shamed into improving their use of encryption.

I want to be clear about something, so that you don't get the wrong impression: Google has put a huge amount of energy and resources into securing the connection between Google and its customers, but Google has done essentially nothing to stop themselves from having access to your data. That means that pre-2009 the NSA or GCHQ could spy on Google users' communications without going to Google, and since the last five years of encryption changes now to get a Google customer's communications, a government must go to Google.

I want to contrast the approach between Google and, say, WhatsApp, which is owned by Facebook, or Apple. Google has made itself the bottleneck for surveillance. If a government,

Deutsche Übersetzung

an ein IT-Unternehmen wenden, werden sie immer den nationalen Telefonanbieter wählen. In vielen Ländern waren die nationalen Telefonanbieter früher staatliche Unternehmen. Sie gehörten möglicherweise zur Postbehörde oder einer anderen Behörde. Sie haben langjährige und tief verwurzelte Beziehungen zum nachrichtendienstlichen Apparat und scheuen keine Mühe, den Regierungen zu Diensten zu sein. Vor 2010 konnten Nachrichtendienste also die E-Mails, SMS und Social-Media-Daten von Nutzern erfassen, ohne sich an Google, Facebook oder Twitter wenden zu müssen. Sie mussten lediglich massenhaft Internetdaten erfassen, sie nach unverschlüsselten Kommunikationen durchsuchen und diese dann auswerten.

2010 begann man in der US-amerikanischen IT-Branche damit, die Daten, die von Nutzern an IT-Unternehmen übermittelt wurden, durch Verschlüsselung zu schützen. Google war in diesem Bereich wahrscheinlich der wichtigste Pionier, aber auch Twitter und Facebook waren ziemlich gut. Yahoo dagegen war ziemlich grauenhaft, bis sie sich nach den Snowden-Enthüllungen gezwungen sahen, endlich ihren Einsatz von Verschlüsselung zu verstärken.

Ich möchte jedoch eines klarstellen, um hier keinen falschen Eindruck entstehen zu lassen: Google hat eine große Menge an Energie und Ressourcen aufgewendet, um die Verbindungen zwischen Google und seinen Kunden zu schützen, aber sie haben im Wesentlichen gar nichts getan, das sie selbst davon abhalten würde, auf Ihre Daten zuzugreifen. Vor 2009 konnten also NSA oder GCHQ die Verbindungen von Google-Nutzern ausspionieren, ohne sich hierzu an Google zu wenden, und seitdem sich die Verschlüsselungspraxis in den vergangenen fünf Jahren geändert hat, muss eine Regierung sich an Google wenden, wenn sie Kommunikationsdaten von Google-Nutzern haben will.

Ich würde gerne hervorheben, wie sich Googles Ansatz hier von dem von, sagen wir, WhatsApp unterscheidet, das zu Facebook gehört, oder von Apple. Google hat sich selbst zum Nadelöhr der

Original

either in Germany or in the U.K. or in the U.S., wants to get a Google customer's communications, because of the security technologies employed by Google, a government must go to Google to get that data now. They can no longer go to their national telephone company for Internet-collected information. In contrast, WhatsApp and Apple have deployed a different form of encryption technology - what's called N2N encryption - which denies themselves access to their users' communications. What that means is that if the U.S. government would like to get the contents of a WhatsApp user's messages, WhatsApp does not have anything of value they can turn over. Those companies are blinding themselves to their users' communications. That is clearly a preferable method, from the perspective of privacy. It does not favor one government over another. Of course, that also means that even in legitimate law enforcement situations, governments are locked out.

Personally, as a technical person, I think that cyber-security trumps the needs of governments, but that is the approach taken by those kinds of companies, and I think we're going to see more and more of that approach as companies finally start to realize that the liability of hosting user data in many cases outweighs the benefits of monetizing user data.

Vorsitzender Dr. Patrick Sensburg: Very interesting. Okay. - Der Nächste ist Kollege Ströbele.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ich habe eine Frage an Dr. Halperin. Sie fünf haben alle eine mehr oder weniger kritische Haltung vertreten gegenüber der Praxis der NSA und haben auch erwähnt und zum Teil auch kritisiert, dass die Maßnahmen, die in den USA nicht nur mit dem FREEDOM Act, sondern

Deutsche Übersetzung

Überwachung gemacht. Wenn eine Regierung, sei es in Deutschland oder Großbritannien oder den USA, an Kommunikationsdaten von Google-Nutzern herankommen will, muss sie sich heute aufgrund der von Google eingesetzten Sicherheitstechnologien an Google wenden. Sie können sich nicht mehr an ihren nationalen Telefonanbieter wenden, um im Internet erfasste Daten zu bekommen. WhatsApp und Apple setzen dagegen eine andere Art von Verschlüsselungstechnologie ein, die sogenannte N2N-Verschlüsselung, die auch diesen Unternehmen selbst den Zugang zu den Kommunikationsdaten ihrer Nutzer verwehrt. Wenn die US-Regierung also Inhalte von WhatsApp-Nachrichten von WhatsApp einfordert, hat WhatsApp nichts von Wert, was es aushändigen könnte. Diese Unternehmen machen sich selbst blind für die Kommunikationsinhalte ihrer Nutzer. Vom Blickwinkel des Datenschutzes aus betrachtet, ist diese Methode die bessere. Sie gibt keiner einzelnen Regierung einen Vorzug. Das bedeutet allerdings natürlich auch, dass den Regierungen auch in rechtmäßigen Strafverfolgungsszenarien der Zugang verwehrt bleibt.

Ich persönlich als IT-Mensch bin der Ansicht, dass Cybersicherheit vor den Bedürfnissen von Staaten kommt. Aber dies ist jedenfalls der Ansatz, den Unternehmen dieser Art verfolgen, und ich denke, wir werden erleben, dass immer mehr Unternehmen diese Herangehensweise übernehmen, wenn sie endlich erkennen, dass die Verpflichtung, die mit dem Hosting von Nutzerdaten einhergeht, in vielen Fällen den Nutzen einer Monetarisierung dieser Daten überwiegt.

Original

auch sonst erfolgen, noch unzureichend sind und dass man mehr machen müsse an Kontrolle und an Einschränkung. Können Sie sagen: Sind Sie in den USA so was wie einsame Rufer in der Wüste, oder ist die Auffassung, die Sie vertreten, eine, die in der Bürgerrechtsszene, in der Menschenrechtsszene, juristischen Szene in den USA verankert ist? Und werden Sie mit Ihren Vorschlägen und Ihrer Kritik beispielsweise auch im Kongress gehört? Werden Sie bei der US-Administration gehört? Also, wie ordnen Sie selber Ihre kritische Haltung insgesamt in den USA ein?

In Deutschland haben viele so ein bisschen die Auffassung, in den USA wird das Verhalten weitgehend für sinnvoll gehalten, dass die NSA so was macht, was ihr vorgeworfen worden ist, und das sei eben notwendig, und dass es eigentlich wenig andere Auffassungen gibt, dass es eine sehr, sehr kritische Haltung - um das mal milde auszudrücken - gegenüber Herrn Snowden gibt. Leute wundern sich dann, wenn ich erzähle, dass es diesen FREEDOM Act zum Beispiel gibt. Wie kann man die Stimmung in den USA, vor allen Dingen in den Kreisen, die sich ernsthaft mit solchen Problemen beschäftigen, einschätzen? Wie weit ist das, was Sie uns hier vortragen, repräsentativ?

Und an Herr Soghoian habe ich die Frage: Sie setzen sich ja sehr für Verschlüsselungen ein, und das ist ja auch ein Rat, den Edward Snowden immer wieder gegeben hat über die Medien: Das soll man weiterentwickeln; man soll möglichst viel verschlüsseln usw. Ich weiß aus dem Jahr 2013 - ich erinnere mich, dass es Meldungen aus den USA gab -, dass einzelnen Firmen, die bestimmte Programme angeboten haben zur Verschlüsselung, besonders effektive Programme angeboten haben - - eine Firma, die ein Programm anbietet oder angeboten hat, das auch Edward Snowden nutzt - der kennt sich ja aus - - dass das verboten worden ist in den USA, dass der Vertrieb einer solchen Software, solcher Programme verboten worden ist. Können Sie sagen: Ist das richtig? Und wie ist die Haltung auch heute dazu? Also, können Sie gut entwickelte

Deutsche Übersetzung

Original

Sicherheitssysteme bedenkenlos in den USA vertreiben? Also, hier war das mal so, dass ich sogar empfohlen habe, solche Firmen sollen, wenn sie in den USA ihre Produkte nicht mehr vertreiben dürfen, doch nach Deutschland kommen, am besten nach Berlin, und das von hier aus machen. Also, können Sie dazu was sagen?

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank für die beiden Fragen. Ich würde sagen, es beginnt Morton Halperin.

Sachverständiger Dr. Morton H. Halperin: So, I was wiretapped by the Nixon administration, and one of my friends said to me, "See, and you said the government was not interested in what you were saying!" So it turns out they may still be interested in what I'm saying. But I think there is some interest in reform. I think the chances for it almost entirely depend on whether a bill is sunsetting. The bulk data was abolished only because the bill was going to be sunsetted. I don't think it would have happened if it was not for that. The FISA Amendments Act has to be renewed, and so I think there will be some changes made. But most of the interest that there is is about the protection of Americans. For example, we've now learned that the government claims the right to go into any of the bulk data that it collects - or what it calls not bulk data - under the FISA Amendments Act to search for information about Americans who it doesn't suspect of any wrongdoing at all. But its argument is, We properly collected this information and therefore we can search through it for information about American citizens. I think Congress is going to fix that. I think it's an outrageous interpretation, and I think Congress is going to fix it when the statute comes up for renewal. There is not, I think, very much interest in the United States in fixing the problem of American spying on the private citizens of other countries. And I think the only way to get interest in that is to link it to limits on surveillance by these foreign intelligence services on American citizens and say, This is a way to stop other countries from spying on American citizens.

Deutsche Übersetzung

Sachverständiger Dr. Morton H. Halperin: *Nun, ich wurde durch die Nixon-Regierung abgehört, und damals sagte ein Freund zu mir: „Siehst du, und du meintest, dass sich die Regierung nicht dafür interessiert, was du sagst! - Wie sich herausstellt, sind sie möglicherweise immer noch daran interessiert, was ich sage. Ich denke jedoch, dass Interesse an einer Reform besteht. Die Chancen dafür hängen meiner Meinung nach fast komplett davon ab, ob eine Gesetzesvorlage ausläuft. Die massenhafte Erfassung und Auswertung von Daten wurde nur deshalb abgeschafft, weil die Gesetzesvorlage auszulaufen drohte. Andernfalls glaube ich nicht, dass es dazu gekommen wäre. Der FISA Amendments Act steht zur Verlängerung an; daher denke ich, dass es einige Veränderungen geben wird. Das bestehende Interesse bezieht sich allerdings zum Großteil auf den Schutz von US-Personen. So haben wir beispielsweise inzwischen erfahren, dass die Regierung das Recht beansprucht, im Rahmen des FISA Amendments Act sämtliche Massendaten, die sie erfasst hat, bzw. die Daten, die sie als nicht massenhaft erfasste Daten bezeichnet, nach Informationen über US-Personen zu durchsuchen, die keinerlei Straftat verdächtigt werden. Die Begründung lautet: Wir haben diese Daten ordnungsgemäß erfasst und dürfen sie daher auch nach Informationen über US-Personen durchsuchen. - Ich denke, der Kongress wird das beheben. Ich halte es für eine ungeheuerliche Situation und denke, dass der Kongress sie beheben wird, wenn das Gesetz zur Verlängerung ansteht. Meiner Meinung nach gibt es in den USA kein großes Interesse an der Lösung des Problems, dass die USA Privatpersonen in*

Original

Sachverständiger Dr. Christopher Soghoian: It is true that until the late 1990s the U.S. government regulated the export of encryption technology, but President Bill Clinton relaxed those controls and weakened the rules so that companies and individual developers could freely distribute encryption technology. There have been encryption tools that have been available for some time, but really in the last five years we've seen a major change in the encryption landscape. Really, it's not that the encryption that is available now is more powerful or suddenly more secure, it's that encryption that is available now is much easier to use.

Five years ago, if you wanted to encrypt your communications, there were tools that were available, and they were free and you could download them online, but they were so difficult to use that the only people who could use them were really the nerds, the tech experts. Probably some of the people in the gallery above us were using things like PGP. But any regular person who has tried to encrypt their email either gives up in frustration or makes mistakes that accidentally make it easier for them to be spied on. That has changed in a really big way. And I think the great irony here is that we probably have to thank Secretary of State Hillary Clinton for the change in the encryption landscape. The U.S. government in the last, I guess, eight years has poured a huge sum of money into the development of easy-to-use secure communications technologies under the guise of Internet freedom. So, the U.S. government, as an act of diplomacy, wished to allow journalists

Deutsche Übersetzung

anderen Ländern ausspionieren. Und ich denke, das einzige Mittel, um hier ein Interesse zu wecken, besteht darin, es mit einer Einschränkung der Überwachung von US-Personen durch die entsprechenden ausländischen Nachrichtendienste zu verbinden und zu sagen: Dies ist eine Möglichkeit, andere Länder davon abzuhalten, amerikanische Staatsbürger auszuspionieren.

Sachverständiger Dr. Christopher Soghoian: *Es ist richtig, dass die US-Regierung bis in die späten 1990er-Jahre den Export von Verschlüsselungstechnologien reguliert hat; aber Präsident Bill Clinton hat diese Handelskontrollen gelockert und die Regelungen geschwächt, sodass Unternehmen und unabhängige Entwickler ihre Verschlüsselungstechnologien frei vertreiben konnten. Es gibt Verschlüsselungstools, die bereits seit einiger Zeit verfügbar sind; aber in den vergangenen fünf Jahren haben wir wirklich eine grundlegende Veränderung in der Verschlüsselungslandschaft beobachtet. Neu ist dabei nicht in erster Linie, dass die heute verfügbaren Verschlüsselungslösungen leistungsstärker oder plötzlich sicherer sind, sondern dass sie sehr viel einfacher zu nutzen sind.*

Wenn man seine Kommunikationsdaten vor fünf Jahren verschlüsseln wollte, hatte man Tools zur Verfügung, die man kostenlos online herunterladen konnte; aber die Nutzung war so kompliziert, dass sie eigentlich nur von den Nerds, den Technik-Spezialisten genutzt werden konnten. Einige der Leute im Zuschauerraum oben haben wahrscheinlich Tools wie PGP genutzt. Aber jeder Normalnutzer, der versuchte, seine E-Mails zu verschlüsseln, hat entweder frustriert aufgegeben oder dabei aus Versehen Fehler gemacht, die dazu führten, dass er noch einfacher ausspioniert werden konnte. Das hat sich inzwischen grundlegend geändert. Und ich denke, die Ironie daran ist, dass wir diese Veränderung der Verschlüsselungslandschaft wahrscheinlich der [früheren] Außenministerin Hillary Clinton zu verdanken haben. Denn die US-Regierung hat in den vergangenen, schätzungsweise acht Jahren unter dem Deckmantel der Internetfreiheit eine

Original

and dissidents in foreign countries to circumvent their national spying apparatus - the filtering by the Great Firewall of China - and so the U.S. government spent a lot of money funding the development of tools like Tor and of a particular messaging encryption technology called Signal. It is not widely known, but I think it is actually something that should be praised, that the encryption that WhatsApp uses - that WhatsApp has delivered to a billion users and that WhatsApp has turned on by default - was actually funded almost entirely with U.S. government money. 2.2 million dollars of U.S. taxpayer funds went to develop this technology. It is extremely easy to use; it was so easy to use that WhatsApp felt comfortable turning it on by default.

Today, any person who uses WhatsApp can protect their communications from basically the most sophisticated actors that are out there. And I think that's really a fantastic development. It's a great return for the American taxpayer; often we do not get as good of a return on 2 million dollars. Taxpayer dollars are unfortunately frequently squandered. This is probably the best return on investment we will ever get for cybersecurity funding. So today strong encryption is not just available on WhatsApp, but on iMessage and Signal, and there are a lot of easy-to-use encryption technologies that are there. What I think is most important to note is that these are turned on by default, so users do not have to seek them out. If you're using a popular service, it's probably turned on.

The last thing I'll note - the representative asked about what is the feeling about these apps, how well are they supported by politicians -: Secretary Clinton is now, as you know, running for

Deutsche Übersetzung

Riesensumme in die Entwicklung nutzerfreundlicher, sicherer Kommunikationstechnologien gepumpt. Als diplomatische Maßnahme wollte es die US-Regierung Journalisten und Dissidenten im Ausland ermöglichen, ihre nationalen Spionageapparate zu umgehen - die Zensur durch die Great Firewall of China. Und daher investierte die US-Regierung sehr viel Geld, um die Entwicklung von Tools wie Tor und die Messaging-Verschlüsselungstechnologie Signal zu fördern. Es ist nicht allgemein bekannt, aber ich halte es für etwas sehr Lobenswertes, dass die Verschlüsselung, die WhatsApp nutzt - die WhatsApp einer Milliarde Nutzern zur Verfügung stellt und standardmäßig aktiviert hat -, fast vollständig durch US-Regierungsgelder finanziert wurde. 2,2 Millionen Dollar US-amerikanischer Steuergelder sind in die Entwicklung dieser Technologie geflossen, die extrem nutzerfreundlich ist. Sie ist so nutzerfreundlich, dass WhatsApp sie ohne Bedenken standardmäßig aktiviert hat.

Heute kann jeder, der WhatsApp benutzt, damit seine Kommunikationsdaten quasi vor den ausgebufftesten Leuten schützen, die es gibt. Und das halte ich für eine wirklich großartige Entwicklung. Es ist eine lohnende Investition von Steuergeldern. So viel bekommen wir nicht oft für 2 Millionen Dollar. Leider werden Steuergelder oft verschleudert. Dies ist wahrscheinlich die beste Rendite, die wir je für eine Finanzierung von Cybersicherheit bekommen werden. Leistungsfähige Verschlüsselungslösungen sind heute also nicht nur bei WhatsApp erhältlich, sondern auch bei iMessage und Signal, und es gibt viele nutzerfreundliche Verschlüsselungstechnologien. Wichtig ist meiner Meinung nach, festzuhalten, dass sie standardmäßig aktiviert sind, sodass die Nutzer sie nicht erst suchen müssen. Wenn man einen beliebten Service benutzt, dann ist die Verschlüsselung wahrscheinlich aktiviert.

Der letzte Punkt, auf den ich eingehen möchte - der Abgeordnete fragte, wie über diese Apps gedacht wird, wie sehr sie durch Politiker unter-

Original

the Presidency. Her campaign is using Signal, it was reported recently, to protect their communications from foreign actors who may be targeting them. And not only that, but both Republican and Democratic members of Congress have been advising their peers to use WhatsApp to secure their communications. In Australia, the Prime Minister there is using WhatsApp to protect his communications, and so I think we're starting to see some politically savvy politicians in different countries realize that their own communications are sensitive and must be secured, and they're looking to the private market for easy-to-use tools to protect them.

Deutsche Übersetzung

stützt werden -: [Die ehemalige] Ministerin Clinton kandidiert, wie Sie wissen, für das Amt der Präsidentin. Wie kürzlich berichtet wurde, verwendet man in ihrer Wahlkampfkampagne Signal, um Kommunikationsdaten vor ausländischen Akteuren zu schützen, die eventuell darauf zuzugreifen versuchen. Darüber hinaus haben Kongressangehörige beider Parteien - Republikaner und Demokraten - ihren Kollegen zur Nutzung von WhatsApp geraten, um ihre Kommunikationsdaten zu schützen. Auch der australische Premierminister nutzt WhatsApp, um seine Kommunikationsdaten zu schützen. Es zeigt sich also langsam, dass politisch intelligenten Politikern in verschiedenen Ländern bewusst wird, dass ihre eigenen Kommunikationsdaten sensibel sind und geschützt werden müssen, und sie schützen diese Daten mit nutzerfreundlichen Tools von Unternehmen aus dem Privatsektor.

Vorsitzender Dr. Patrick Sensburg: Ja, ganz herzlichen Dank. - Wir kommen zur nächsten Frage, die der Kollege Hahn stellt.

Dr. André Hahn (DIE LINKE): Ich kann gleich anschließen an das Letzte, was eben gesagt worden ist bezüglich des Schutzes von Parlamentariern und anderen vor solcher Ausspähung. Da möchte ich vielleicht mal konkret fragen: Der Deutsche Bundestag hat ja über viele Jahre, über etliche Jahre als Betreiber der Telekommunikationsanlage Verizon gehabt. Nach dem, was Sie wissen: Ist denn davon auszugehen, dass dann, wenn das der Fall war und die Kontakte ja auch zum Mutterunternehmen, zu den USA, da sind, die gesamte Kommunikation des Parlamentes und anderer, die daran angeschlossen waren, auch an die NSA gegangen ist? Wie ist da Ihre Bewertung, wenn Sie das vielleicht sagen könnten?

Die zweite Frage schließt an das an, was Kollege Flisek schon gefragt hat. Da weiß ich jetzt noch nicht konkret, wem ich die zuordnen soll, ehrlich gesagt; da wäre ich dann dankbar, wenn jemand vielleicht was dazu sagen könnte. - Es gibt ja eine offizielle Kooperation zwischen BND und

Original

NSA. Es gibt Verträge; es gibt gemeinsame Operationen. Und ich habe die Frage vorhin so verstanden: Wie viel an NSA-Tätigkeit in Deutschland ist Kooperation, ist abgesprochen mit Wissen der Bundesregierung möglicherweise, und wie viel von dem, was die NSA hier in Deutschland macht, wie viel Prozent ist überhaupt nicht im Rahmen von Kooperationen, von gemeinsamen Aktivitäten, sondern eben aus unserer Sicht auch illegal, also von dem, was die NSA hier tut? Kann man das irgendwie quantifizieren? Und was macht die NSA hier nach Ihrer Kenntnis? Geht sie an Glasfaser? Was passiert hier? Was macht die NSA tatsächlich in Deutschland?

Vorsitzender Dr. Patrick Sensburg: Okay. Jetzt müssten wir nur noch wissen, wer die erste Frage beantwortet. - Bitte? Die erste Frage war an wen? Mr. Soghoian?

Dr. André Hahn (DIE LINKE): Mr. Soghoian.

Vorsitzender Dr. Patrick Sensburg:
Mr. Soghoian. - Okay, Mr. Soghoian.

Sachverständiger Dr. Christopher Soghoian: So if the only thing protecting your parliamentary communications is the nationality of the company that is transiting those communications, whether a U.S. company or a Belgian company or a German company, you're in trouble. You need to use more than just a flag to protect your communications. You must use encryption technology. I will ask you, and I hope that you can respond: Do you have the ability, as a Member of Parliament, to make an encrypted telephone call to your peers? Do you regularly make encrypted telephone calls to your peers, or are most of your communications done over unencrypted telephone lines?

We have to remember: the embassies of the U.S. government and the U.K. government are just a few blocks away from here. We know that the

Deutsche Übersetzung

Sachverständiger Dr. Christopher Soghoian: *Wenn die Nationalität des Unternehmens, das Ihre parlamentarischen Kommunikationsinhalte übermittelt - sei es nun amerikanisch, belgisch oder deutsch - das Einzige ist, was diese Kommunikationsinhalte schützt, dann haben Sie ein Problem. Sie brauchen mehr als eine Flagge, um Ihre Kommunikationsdaten zu schützen. Sie müssen Verschlüsselungstechnologie einsetzen. Ich möchte Sie fragen und hoffe, dass Sie meine Frage beantworten können: Haben Sie als Abgeordnete die Möglichkeit, verschlüsselte Telefonate mit Ihren Kollegen zu führen? Führen Sie regelmäßig verschlüsselte Telefonate mit Ihren Kollegen, oder erfolgt der Großteil Ihrer Kommunikation über unverschlüsselte Telefonverbindungen?*

Vergessen wir nicht, dass die US-amerikanische und die britische Botschaft nur einen Katzensprung entfernt liegen. Wir wissen, dass der Special Collection Service, eine Spezialeinheit

Original

Special Collection Service, the NSA's unit, operates out of their embassy, where they have a spy mast. We know that the U.K. government has a spy mast in their embassy. And, of course, the Chinese and the Russians are almost certainly doing the same thing. The U.S. government is not restricted to only spying with the help of U.S. companies. We know, for example, that intelligence services hack into foreign telecommunications companies. The hack by GCHQ of Belgacom, one of Belgium's largest phone companies, is well known at this point. And so if the German parliament were to entrust your communications to Belgacom, the NSA and GCHQ would have had them, because they have penetrated the core network of Belgacom.

You must employ strong security technologies. You cannot use personally managed cell phones, you cannot use personal email accounts to conduct parliamentary business, and you must dedicate significant resources to computer security. In the United States, our own government is learning this the hard way after the communications of political parties have been penetrated by what we have been told is the Russian government. Security must be a priority, and you can only rely on security technology to protect your communications from foreign governments, not a contract with a telecommunications carrier.

Vorsitzender Dr. Patrick Sensburg: Die zweite Frage war sehr offen gehalten. Ich weiß nicht, wer sich berufen fühlt. Vielleicht Frau Stepanovich? „Was macht die NSA bei uns?", so fasse ich es mal in einem Satz zusammen. Wenn Sie es können.

Sachverständige Amie Stepanovich: I think the only proper answer to that question is that we don't know. The agreements between Germany and the United States are secret, just like the

Deutsche Übersetzung

der NSA, von der Botschaft aus arbeitet und dort eine Abhöranlage betreibt. Wir wissen, dass auch die britische Regierung eine Abhöranlage auf ihrem Botschaftsgebäude hat. Und natürlich tun die Chinesen und die Russen mit an Sicherheit grenzender Wahrscheinlichkeit genau dasselbe. Die US-Regierung ist nicht darauf beschränkt, nur mit der Hilfe von US-Unternehmen zu spionieren. Wir wissen beispielsweise, dass sich Geheimdienste in die Netzwerke ausländischer Telekommunikationsanbieter einhacken. Der Fall von Belgacom, einer der größten belgischen Telefongesellschaften, deren Netzwerk vom GCHQ gehackt wurde, ist mittlerweile allgemein bekannt. Falls also der Deutsche Bundestag seine Kommunikationsdaten Belgacom anvertrauen würde, hätten NSA und GCHQ diese Daten, denn sie sind in das Kernnetzwerk von Belgacom eingedrungen.

Sie müssen also leistungsstarke Sicherheitstechnologien einsetzen. Sie dürfen keine privaten Mobiltelefone oder privaten E-Mail-Accounts für parlamentarische Angelegenheiten nutzen, und Sie müssen bedeutende Ressourcen für die Computersicherheit bereitstellen. Unsere Regierung in den Vereinigten Staaten musste in dieser Beziehung viel Lehrgeld zahlen und hat erst reagiert, als Server der politischen Parteien durch, wie uns gesagt wurde, den russischen Geheimdienst gehackt wurden. Sicherheit muss zur Priorität werden, und Sie können Ihre Kommunikationsdaten nur durch Sicherheitstechnologie vor ausländischen Regierungen schützen, nicht durch Verträge mit Telekommunikationsnetzbetreibern.

Sachverständige Amie Stepanovich: *Ich denke, die einzig zutreffende Antwort auf diese Frage lautet: Wir wissen es nicht. Die Abkommen zwischen Deutschland und den Vereinigten Staaten*

Original

agreements between the U.S. National Security Agency and other countries. And it is unclear to the extent that that cooperation is happening. If you wanted to look instead at the extent that the NSA *could* be conducting surveillance in Germany and has the authority to, I think it is very clear that they have very wide authority to do that under EO 12333, as has been previously explained, not only of regular citizens in Germany but also Members of Parliament, in order to collect foreign intelligence information, under that very broad definition that Ms. Gorski gave. And so we, without any information about the extent of those agreements, both directly between the United States and Germany as well as within the broader scope of the 41 Eyes - I believe it's the largest organization of countries - and then further down from there all the way to the organizations that Germany is not a member of, we have been putting a tremendous amount of pressure on governments to try to release some information about those agreements. Privacy International, another civil society organization, has done a very good job. I reference this in my written testimony, trying to document what is in those agreements. Unfortunately, far too much information is not available on this inter-government coordination and cooperation. And it is probably the area of our national security surveillance that we know the least about.

Deutsche Übersetzung

sind geheim, ebenso wie die Abkommen zwischen der U.S. National Security Agency und anderen Staaten. Und es ist unklar, welchen Umfang diese Zusammenarbeit hat. Wenn man sich dagegen ansieht, in welchem Ausmaß die NSA Überwachungen in Deutschland durchführen könnte und dazu auch befugt ist, dann wird meiner Ansicht nach sehr deutlich, dass sie hierzu nach EO 12333 eine sehr weitreichende Befugnis hat, wie bereits erläutert wurde. Und das betrifft nicht nur die Überwachung von Normalbürgern in Deutschland, sondern auch von Mitgliedern des Deutschen Bundestages mit dem Ziel, Daten für die Auslandsaufklärung zu erfassen, und zwar entsprechend der sehr weitgefassten Definition, die Frau Gorski genannt hat. Ohne jede Information darüber, wie weit diese Abkommen reichen - sowohl die direkten Abkommen zwischen den USA und Deutschland als auch die Abkommen im breiteren Umfeld der 41 Eyes, des meines Wissens größten Zusammenschlusses von Staaten, und auch der Zusammenschlüsse, denen Deutschland nicht angehört - haben wir enormen Druck auf Regierungen ausgeübt, um zumindest einige Informationen über diese Abkommen öffentlich zu machen. Privacy International, eine weitere zivilgesellschaftliche Organisation, hat hier sehr gute Arbeit geleistet. In meiner schriftlichen Stellungnahme beziehe ich mich darauf und habe versucht, zu dokumentieren, was diese Abkommen enthalten. Leider liegen uns viel zu wenig Informationen zu dieser zwischenstaatlichen Koordination und Zusammenarbeit vor. Es ist vermutlich der Bereich unserer staatlichen geheimdienstlichen Überwachung, über den wir am wenigsten wissen.

Vorsitzender Dr. Patrick Sensburg: Okay. Ich glaube, es wird noch Nachfragen in dieser Richtung geben. - Als Nächstes ist die Kollegin Warken dran.

Nina Warken (CDU/CSU): Zunächst vielen Dank an Sie alle, dass Sie uns heute hier zur Verfügung stehen und wir die Gespräche, die wir in den USA begonnen haben mit einigen von Ihnen, fortsetzen können.

Original

Ich habe zwei Fragen an Herrn Edgar. Zum einen: Können Sie vielleicht noch mal ausführen, was sich konkret geändert, verbessert hat im Bereich der gerichtlichen und parlamentarischen Kontrolle, im Bereich der Aufsicht?

Und dann auch anknüpfend an das, was vorhin schon gefragt wurde im Bereich Abkommen zwischen Ländern - der Kollege Flisek hatte nach No-Spy gefragt -: Wie ich das verstanden habe, sehen einige es als eher unrealistisch, dass es ein No-Spy im Sinne eines kompletten Verzichts gibt, aber dass - so hatten Sie das gesagt, Herr Edgar - bei Kooperationen ja vereinbart werde, dass die Staatsbürger gegenseitig geschützt sind. Ist das bei den Five Eyes generell so aus Ihrer Sicht, und ist es sozusagen die Grundlage oder die Keimzelle dessen, worauf sich dann internationale Vereinbarungen stützen könnten, also den Bürgerschutz?

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Herr Edgar.

Sachverständiger Timothy H. Edgar: Thank you, Ms. Warken. I didn't catch the very beginning of your first question because my translator was mis-functioning, but I believe it was about judicial oversight? - Okay.

So, as I explain further in my paper, my view is that we have seen through the experience of Section 702 of FISA, which many of my colleagues have been quite critical of, that there is actually a positive outcome of that, which is: it's the first example of a large-scale NSA program being subjected to any kind of judicial oversight at all. The Foreign Intelligence Surveillance Court was set up, very much like the G 10 Commission here, to review individual targets under a standard of probable cause. And in that respect it operated very much like an ordinary court, although a secret one. With Section 702 of FISA, it really is looking at a broad program of what you might call mass surveillance, and analyzing the safeguards and procedures that the agency is using, and then if those procedures are violated,

Deutsche Übersetzung

Sachverständiger Timothy H. Edgar: *Vielen Dank, Frau Warken. Ich habe den Anfang Ihrer ersten Frage nicht ganz verstanden, weil die Übersetzung nicht funktioniert hat, aber es ging, wenn ich richtig liege, um die gerichtliche Kontrolle? - Okay.*

Nun, wie ich in meinem schriftlichen Beitrag näher ausführe, bin ich der Ansicht, dass die Erfahrungen mit § 702 des FISA, zu dem sich viele meiner Kollegen sehr kritisch geäußert haben, gezeigt haben, dass es uns doch auch etwas Positives beschert hat: Es ist das erste Beispiel für ein großangelegtes NSA-Programm, das überhaupt irgendeiner gerichtlichen Kontrolle unterstellt ist. Das Foreign Intelligence Surveillance Court wurde, ganz ähnlich wie hier die G 10-Kommission, eingerichtet, um einzelne Fälle von Überwachungen von Zielpersonen nach dem Grundsatz des hinreichenden Tatverdachts zu prüfen. In dieser Beziehung handelte es sehr ähnlich wie ein normales Gericht, auch wenn es geheim war. Nach § 702 des FISA be-

Original

figuring out remedies. And it did that on several occasions involving Section 702.

So it's my contention that this shows that judges can actually play a useful role in overseeing not just individual targeted surveillance but also broader surveillance programs, and that they can provide rigor where just an internal compliance office provides less rigor. If I violate the rules that the FISA Court has given me in Prism or Upstream collection, I violate a court order, I potentially violate the law, and I could suffer criminal penalties. If I violate the rules in EO 12333 or in Presidential Policy Directive 28, I don't violate the law; I do violate the rules and I could be subject to internal discipline - and in fact many people have been disciplined under those provisions -, but it's less rigorous than having a law that's enforced by a court.

So, that's point number one, that I think we should have judicial oversight, at least within the American system, of pretty much everything that the NSA does. And that would include things that they are doing together with the BND on German territory as well as what they would do in the United States when it comes to Prism or Upstream collection in very much the same way.

And that leads me to your second question about - which we've been discussing - the idea of what exactly is the Five Eyes agreement. Does it mean that we don't agree to spy on each other? And what would it mean to extend similar kinds

Deutsche Übersetzung

trachtet es wirklich ein breitgefasstes Überwachungsprogramm, das man auch als massenhafte Überwachung bezeichnen könnte, und analysiert die Schutzvorkehrungen und Verfahren, die vom Nachrichtendienst angewendet werden. Und wenn gegen diese Verfahren verstoßen wird, sucht das FISC nach geeigneten Rechtsmitteln. Dies hat es bereits in mehreren § 702 betreffenden Fällen getan.

Ich würde also behaupten, dass sich hier zeigt, dass Richter tatsächlich eine hilfreiche Rolle in der Aufsicht von Überwachungsprogrammen spielen können, und zwar nicht nur bezüglich der gezielten Einzelüberwachung, sondern auch bei breiter angelegten Programmen, und dass sie mehr Durchsetzungskraft haben als nur eine interne Compliance-Stelle. Wenn ich gegen die Regelungen des Foreign Intelligence Surveillance Court zu Prism oder Upstream-Überwachung verstoße, dann breche ich damit möglicherweise das Gesetz und muss mit entsprechenden strafrechtlichen Sanktionen rechnen. Wenn ich jedoch gegen die Vorgaben von EO 12333 oder der Presidential Policy Directive 28 verstoße, breche ich damit kein Gesetz. Ich verstoße gegen die Vorgaben und muss mit einem internen Disziplinarverfahren rechnen, und es wurden im Rahmen dieser Vorgaben tatsächlich Disziplinarverfahren gegen Mitarbeiter geführt. Doch das alles ist weniger konsequent und streng als ein Gesetz, das von einem Gericht durchgesetzt wird.

Das wäre also der erste Punkt: Ich denke, es sollte zumindest im US-amerikanischen System eine gerichtliche Kontrolle über so ziemlich alles geben, was die NSA tut. Und das würde auch gemeinsame Aktivitäten mit dem BND auf deutschem Staatsgebiet einschließen, ebenso wie die Aktivitäten im Zusammenhang mit Prism und Upstream-Datenerfassung.

Und damit komme ich auch zu Ihrer zweiten Frage zu dem bereits besprochenen Konzept des Five-Eyes-Abkommens und was das genau ist. Ob es bedeutet, dass wir nicht darüber übereinkommen, einander auszuspionieren und was es

Original

of - - Could we enlarge that group or somehow increase the protections that are available to other NSA partners?

My first point would be that, as a technical matter, the government has actually been clear that the Five Eyes agreement is not, strictly speaking, a no-spy partnership, although I think that in practice it amounts to the same thing, and I'll explain why. The agreement does not say, we won't spy on each other. What it says is that the participants in the Five Eyes will share signals intelligence with each other. That includes data, that includes techniques and tactics, it includes basically working together to gather large amounts of information around the world very seamlessly. And, in fact, inside the intelligence community, it was sometimes commented that on occasion it was much easier to share intelligence with the British or with the Canadians than even with our own government, within individual agencies within our own government. Just because of the way classification rules worked.

So that gives you a sense of just how close this partnership is. And it doesn't include a commitment not to spy on each other, but in practice that amounts to almost the same thing, because if you were going to engage in some kind of program directed against the British, for example, you would not really physically be able to do it, because of the closeness of the partnership between those two services. So, that's how that kind of works.

And then the question is, how does that work with other partners and other countries? And that goes back to a question that Mr. Ströbele asked about, "Well, what is the BND actually doing here in Germany with the NSA?" And here I want to be very careful to choose my words carefully. But essentially the operations that the NSA has anywhere in the world can be

Deutsche Übersetzung

eine Ausweitung ähnlicher - - Könnten wir die Gruppe erweitern oder den Schutz von anderen NSA-Partnern irgendwie verstärken?

Erstens würde ich sagen, dass die Regierung auf der theoretischen Ebene klar gesagt hat, dass das Five-Eyes-Abkommen strenggenommen kein No-Spy-Abkommen ist, wobei ich der Meinung bin, dass es praktisch auf dasselbe hinausläuft, und ich erkläre auch, warum. Im Abkommen heißt es nicht, dass die Partner einander nicht ausspionieren werden. Es heißt dort, dass die Mitglieder der Gruppe der Five Eyes ihre Signalaufklärung miteinander teilen. Das umfasst Daten, Techniken und Strategien. Es heißt im Grunde, dass man zusammenarbeitet, um sehr nahtlos große Mengen an Informationen in der ganzen Welt zu erfassen. Und tatsächlich hieß es innerhalb der Geheimdienstkreise schon manchmal, dass es in manchen Fällen viel leichter sei, Informationen zum Beispiel mit den Briten oder den Kanadiern zu teilen als mit unserer eigenen Regierung, also zwischen einzelnen Nachrichtendiensten unserer Regierung. Das lag einfach an dem System der Geheimhaltungsregeln.

Das sollte Ihnen einen Eindruck darüber vermitteln, wie eng diese Partnerschaft ist. Sie umfasst zwar keine Verpflichtung, einander nicht auszuspionieren, aber in der Praxis läuft es fast auf dasselbe hinaus; denn wenn man beispielsweise vorhätte, ein Spionageprogramm gegen die Briten durchzuführen, wäre man dazu rein praktisch gar nicht in der Lage, weil die Partnerschaft zwischen den beiden Geheimdiensten einfach zu eng ist. So ungefähr funktioniert das also.

Die nächste Frage ist, wie es mit anderen Partnern und Staaten funktioniert. Damit beziehe ich mich auch auf eine Frage von Herrn Ströbele, der fragte, was der BND hier in Deutschland eigentlich mit der NSA tut. Und ich versuche, mich hier möglichst vorsichtig auszudrücken, doch im Wesentlichen lassen sich die Aktivitäten der NSA in der ganzen Welt in zwei Arten unterteilen: Entweder handelt es sich um

Original

categorized in two ways: either these are cooperative operations together with the intelligence service of a friendly country, or they're what's called unilateral operations, which is essentially espionage, spying, which, in the latter case, would typically be quite risky, from the government's perspective. It is most likely illegal under that country's laws. It could violate diplomatic understandings. It could affect the relationship between those two countries in a negative way. And so there should be, and typically is, a high bar for engaging in those kinds of operations.

One of the things we've learned from the Snowden revelations is that the NSA, at least prior to 2013, was engaged in operations that I would say the risk exceeded any value of the operation. If I want to know what the Chancellor of Germany thinks about something and I'm the President of the United States, it's probably a good idea to just get on the phone and call her and ask her what she thinks. And we have a relationship with Germany where that generally works pretty well. So, with other countries you can imagine a situation where it's more tense and where the government of that foreign country might be a government where the value of the foreign intelligence would be high. Of course, the value of foreign intelligence of any large country including Germany is high, but you have to look at the risk of operations that could affect the relationship between those two countries.

So, I guess I would turn the question a little bit back on to this committee and say to you all that those are exactly the kinds of questions that I would expect. If I were a German citizen I would want my government to be asking those questions of the United States government. I would want them to be asking, "Okay, we have a partnership with you in many areas, including intelligence. Do we benefit from that partnership?" I would say, absolutely. Germany is getting a lot of information about terrorism and other threats that are common to Germany and the United

Deutsche Übersetzung

Kooperationen mit dem Nachrichtendienst eines befreundeten Landes oder um sogenannte unilaterale Operationen, also im Grunde um Spionage. Letztere ist im Normalfall aus Sicht der Regierung ziemlich risikobehaftet. Höchstwahrscheinlich ist sie dem Gesetz des betreffenden Landes zufolge unrechtmäßig. Sie könnte gegen diplomatische Vereinbarungen verstoßen. Sie könnte die Beziehungen zwischen den beiden Ländern negativ beeinflussen. Und daher sollte die Schwelle für die Durchführung solcher Operationen sehr hoch sein und ist es normalerweise auch.

Eines der Dinge, die wir dank der Snowden-Enthüllungen wissen, ist, dass die NSA, zumindest vor 2013 Operationen durchführte, bei denen das Risiko meiner Ansicht nach jeden möglichen Wert des Ergebnisses überwog. Wenn ich als Präsident der Vereinigten Staaten gerne wissen möchte, was Bundeskanzlerin Merkel zu einer bestimmten Frage denkt, dann ist es wahrscheinlich eine gute Idee, sie einfach anzurufen und zu fragen. Unsere Beziehungen zu Deutschland sind so, dass das im Allgemeinen ganz gut funktioniert. Bei anderen Staaten kann man sich eine Situation vorstellen, die etwas angespannter ist, mit einer Regierung, bei der der Wert der Auslandsaufklärung hoch wäre. Natürlich ist der Wert der Auslandsaufklärung in jedem größeren Land, auch in Deutschland, hoch, aber man muss ihn gegen das Risiko aufwiegen: dass die geheimdienstlichen Aktivitäten die Beziehung zwischen den Ländern beeinträchtigen könnten.

Ich denke also, ich würde die Frage gerne an diesen Ausschuss zurückgeben und Ihnen sagen, dass genau dies die Art von Fragen ist, die ich erwarten würde. Wenn ich deutscher Staatsbürger wäre, würde ich mir wünschen, dass meine Regierung der US-Regierung diese Fragen stellt. Ich würde mir wünschen, dass sie fragt: Unsere Partnerschaft mit Ihnen umfasst viele Bereiche, auch die Aufklärung. Profitieren wir von dieser Partnerschaft? - Meine Antwort wäre: Unbedingt! - Deutschland erhält sehr viele Informa-

Original

States. And then the question is, "What kind of restrictions, what kind of rules do we think should govern our partnership with you in the United States?" And you could look at the rules for the Five Eyes, and you could say, "If this is the gold standard, you know, we'd like something close to that, please, because we are such close allies in so many areas." And I think that would be a legitimate question to ask.

And the final point I would say is, you know, why does the United States want this partnership with Germany? Well, I'd say there are a lot of very good reasons why the United States wants to have a close intelligence partnership with Germany: just the size of the country, the sophistication of its intelligence and military services. And the fact that Germany is in the middle of Europe makes a difference when it comes to gathering intelligence, whether that's from satellites or cables. So, obviously the United States benefits significantly from this partnership as well.

So, Germany has some cards that it can use to play. It has some leverage over the United States in this relationship, and of course the United States has leverage as well, because Germany benefits from the partnership as well. And I think what Dr. Halperin and I have really been saying is, we are hoping to kind of raise the bar for everyone. That our process of reform is something you can learn from PPD-28 and some of the greater transparency, the Freedom Act. We can also learn from you, and as these friendly countries raise the bar for our intelligence services, we can really create a situation in which we can have more confidence that whatever these services are doing in cooperation with each other follows certain rules and principles that make sense. I think that's it.

Deutsche Übersetzung

tionen zum Terrorismus und zu anderen Bedrohungen, die Deutschland und die Vereinigten Staaten betreffen. Und die nächste Frage wäre dann: „Welche Einschränkungen, welche Regeln sollten in den Vereinigten Staaten für unsere Partnerschaft mit Ihnen gelten?" Und hier könnten Sie sich die Regeln der Five Eyes ansehen und sagen: Wenn dies der Goldstandard ist, dann hätten wir bitte gerne etwas, das dem sehr nahe kommt, denn wir sind schließlich in so vielen Bereichen so enge Verbündete. - Ich denke, das wäre eine berechtigte Frage.

Der letzte Punkt ist wohl die Frage, warum die USA diese Partnerschaft mit Deutschland möchten. Nun, ich würde sagen, es gibt viele gute Gründe, weshalb die USA an einer engen nachrichtendienstlichen Partnerschaft mit Deutschland interessiert sind. Allein schon die Größe des Landes und der hohe Entwicklungsstand seines Militärs und seiner Nachrichtendienste. Auch die Tatsache, dass Deutschland in der geografischen Mitte Europas liegt, ist für die Informationsbeschaffung von Belang, sei es über Satellit oder durch Kabel. Also profitieren die Vereinigten Staaten auch ganz erheblich von dieser Partnerschaft.

Deutschland hat also einige Trümpfe in der Hand. Es hat in dieser Beziehung einen gewissen Einfluss, und natürlich haben auch die USA einen Einfluss, denn Deutschland profitiert ebenfalls von der Partnerschaft. Und ich denke, was Dr. Halperin und ich sagen möchten, ist, dass wir die Messlatte für alle anzuheben hoffen. Dass Sie etwas aus unserem Reformprozess lernen können - aus der PPD-28 und zum Teil auch aus der größeren Transparenz, dem Freedom Act. Auch wir können etwas von Ihnen lernen, und wenn die befreundeten Länder die Messlatte für ihre und unsere Nachrichtendienste höher legen, können wir eine Situation schaffen, in der wir mehr Vertrauen darin haben können, dass das, was diese Geheimdienste gemeinsam tun, bestimmten Regeln und sinnvollen Grundsätzen folgt. Ich denke, das ist alles.

Original

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Wir kommen jetzt zu den nächsten Fragen. Der Kollege Flisek mit seinen Fragen.

Christian Flisek (SPD): Danke. - Ich würde zunächst einmal noch eine Frage an Frau Gorski stellen wollen. Und zwar würde ich Ihnen ganz gerne zur Einleitung dieser Frage ein Zitat vorlesen, das aus einem Interview Edward Snowdens mit dem Norddeutschen Rundfunk stammt, namentlich mit Herrn Hubert Seipel. Das wurde ausgestrahlt am 26. Januar 2014. Und Edward Snowden sagte dort - ich zitiere; das ist die deutsche Übersetzung, die ich jetzt vorlese -:

> Es gibt keine Zweifel, dass die USA Wirtschaftsspionage betreiben. Wenn es bei Siemens Informationen gibt, von denen sie meinen, dass sie für die nationalen Interessen von Vorteil sind, nicht aber für die nationale Sicherheit der USA, werden sie der Information hinterherjagen und sie bekommen.

Ich würde Sie ganz gerne jetzt fragen, ob Sie diese Aussage von Herrn Snowden für glaubwürdig halten, ob Sie sagen: Ja, genau so, wie er es hier skizziert hat, ist es. - Und was wäre, wenn das so wäre? Was wäre dann der Unterschied aus Ihrer Sicht zwischen dieser Differenzierung, einerseits Verfolgung nationaler Interessen der USA und der anderen Kategorie, Maßnahmen zu ergreifen, die für die nationale Sicherheit von Bedeutung sind? Also, umgekehrt gefragt: Ist denn die NSA jenseits von Aktivitäten, die der nationalen Sicherheit dienen, befugt, auch Maßnahmen zu ergreifen, die, ich sage jetzt mal allgemein, von nationalem Interesse sind, whatever that is? Also, das wäre mal grundsätzlich der Ansatzpunkt.

Dann würde ich Sie gerne auch fragen: Wenn das so wäre, würde dann die NSA befugt sein, solche Erkenntnisse, die auf nachrichtendienstlichem Wege erlangt worden sind, auch poten-

Deutsche Übersetzung

Original

ziellen Wettbewerbern in den USA weiterzugeben? Beziehungsweise halten Sie so was für möglich?

Wir haben ja auch eine Aussage des derzeitigen US-Präsidenten Barack Obama, der Anfang 2014 gesagt hat, die USA betrieben keine Wirtschaftsspionage gegen ausländische Unternehmen. Da würde ich Sie gerne fragen, wie Sie diese Aussage des US-Präsidenten im Kontext dieses Zitats von Edward Snowden, das ich Ihnen gerade vorgelesen habe, sehen.

Dann hätte ich an Herrn Soghoian eine Frage. Also, ich würde Ihnen eigentlich ganz gerne eine Frage stellen, die wir immer gestellt bekommen als Parlamentarier, wenn wir Veranstaltungen mit Bürgern irgendwo in Deutschland zu unserer Arbeit hier im Untersuchungsausschuss machen. Es taucht immer eine Frage auf - ich nehme das jetzt mal auf mich bezogen -: Herr Flisek, glauben Sie, dass Sie abgehört werden? - Jetzt würde ich Sie mal fragen: Unter dem Themenbereich der politischen Spionage, gehen Sie davon aus, dass die NSA, ich sage mal, die Mitglieder, vielleicht die Obleute, den Vorsitzenden dieses Untersuchungsausschusses abhört?

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Wir fangen mit Frau Gorski an.

Sachverständige Ashley Gorski: Thank you. - You asked whether the NSA is engaged in surveillance that goes beyond national security. And I'll answer that question first. Ah, yes! The answer is absolutely yes. Given the definition of foreign intelligence in Section 702, which encompasses the foreign affairs of the United States, there can be no doubt that the surveillance goes beyond simply national security. And, as I noted, the definition of foreign intelligence in EO 12333 is even broader. Under the executive order, foreign intelligence is defined as

Deutsche Übersetzung

Sachverständige Ashley Gorski: *Vielen Dank. Sie fragten, ob die NSA auch über den Bereich der nationalen Sicherheit hinaus Überwachungen durchführt, und ich werde diese Frage als erste beantworten. Ja, allerdings. Die Antwort lautet unbedingt: Ja. Angesichts der Definition des Begriffs Auslandsaufklärung in § 702, die auch die ausländischen Angelegenheiten der Vereinigten Staaten betrifft, besteht kein Zweifel daran, dass die Überwachung über den Bereich der nationalen Sicherheit hinausgeht. Und, wie ich bereits anmerkte, definiert EO 12333 den Begriff Auslandsaufklärung noch breiter. In der Executive Order wird Auslandsaufklärung definiert als:*

Nur zur dienstlichen Verwendung

Original

> … information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

So, under the executive order, legitimate foreign intelligence is information related to the capabilities, intentions or activities of foreign persons, full stop.

You then asked about Edward Snowden's statement in January 2014 that there can be no doubt that the U.S. is in the business of industrial espionage. Based on my understanding of the Snowden disclosures and certain leaks, that appears to have been true. However, I would note that with PPD-28 and the accompanying Section 4 procedures that the NSA issued to implement PPD-28 in January 2015, there was a clarification about the scope of legitimate foreign intelligence information that relates to what you might term industrial espionage. And there the NSA's revised procedures state that:

> The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies.

Specifically:

> It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially.

Deutsche Übersetzung

> *… Informationen zu den Möglichkeiten, Absichten oder Aktivitäten ausländischer Regierungen oder Teilen davon, von ausländischen Organisationen, von Einzelpersonen oder zu internationalen terroristischen Aktivitäten.*

Der Executive Order zufolge umfasst die rechtmäßige Auslandsaufklärung also Informationen, die sich auf die Möglichkeiten, Absichten oder Aktivitäten ausländischer Personen beziehen. Punkt.

Sie fragten auch nach Edward Snowdens Aussage vom Januar 2014, in der er sagte, es bestehe kein Zweifel daran, dass die USA Industriespionage betreiben. Meinem Verständnis der Snowden-Enthüllungen und bestimmter Leaks zufolge scheint diese Aussage richtig gewesen zu sein. Dabei würde ich jedoch anmerken, dass im Zusammenhang mit der PPD-28 und den dazugehörigen Verfahren gemäß § 4, die die NSA im Januar 2015 einführte, um die Direktive 28 umzusetzen, eine Klärung stattgefunden hat, was den legalen Rahmen der Auslandsaufklärung betrifft, die man als Industriespionage bezeichnen könnte. Die überarbeitete Verfahrensrichtlinie der NSA erklärt hier:

> *Die Erfassung von vertraulichen geschäftlichen Daten oder Betriebsgeheimnissen ist nur zum Schutz der nationalen Sicherheit der Vereinigten Staaten von Amerika oder ihrer Partner oder Bündnispartner gestattet.*

Insbesondere heißt es dort:

> *Die Erfassung solcher Informationen mit dem Ziel, US-Unternehmen bzw. US-Unternehmenssektoren einen wirtschaftlichen Wettbewerbsvorteil zu verschaffen, stellt keinen zulässigen Zweck der Auslandsaufklärung oder Spionageabwehr dar.*

Original

However:

> Certain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage.

So, I think there is an effort here, in this document, to mitigate industrial espionage, but at the same time the devil is in the details and it's difficult to say how exactly these standards are being applied by the U.S. government today. They certainly contemplate foreign intelligence surveillance for the purpose of identifying sanctions violations and government influence or direction, which is a very broad term.

Sachverständiger Dr. Christopher Soghoian: You asked me whether I think that you are being spied on, and other members of the committee. I guess I'll turn the question back to you and say: How important are you? No, but to be serious for a moment: the NSA receives tasking orders from other parts of the government. So, if the Secretary of State says that she or he would like to learn what members of the German parliament are doing, then NSA will go and collect the communications of the German parliament. If the Treasury Department or the President wants that information, then they will go and get it. For the most part, NSA works for other parts of the government; it has clients.

And so the real question is: Are your communications of interest to the parts of the U.S. government that have the authority to task collection? Now, I suspect that at least some members of the German parliament are being monitored by the NSA, and I think the question as to whether you are being monitored or specifically tasked is going to depend on what you're working on, which legislative areas you're involved in, and, to be perfectly frank, how good or bad your personal security is. If you make it easy for the Americans

Deutsche Übersetzung

Allerdings:

> *Bestimmte wirtschaftliche Zwecke, zum Beispiel die Feststellung von Handels- oder Sanktionsverstößen oder von staatlicher Einflussnahme oder Lenkung, gelten nicht als Wettbewerbsvorteil.*

Ich denke also, dass man mit diesem Dokument bestrebt war, die Industriespionage abzuschwächen; doch gleichzeitig steckt hier der Teufel im Detail, und es ist schwer zu sagen, wie diese Normen heute im Einzelnen von der US-Regierung angewendet werden. Denn es wird darin auf jeden Fall die Überwachung in der Auslandsaufklärung zu dem Zweck in Erwägung gezogen, Sanktionsverstöße sowie staatliche Einflussnahme und Lenkung festzustellen, und das ist eine sehr weitgefasste Formulierung.

Sachverständiger Dr. Christopher Soghoian: *Sie fragten mich, ob ich glaube, dass Sie und andere Mitglieder dieses Komitees abgehört werden. Ich denke, ich stelle die Gegenfrage: Wie wichtig sind Sie? Doch im Ernst: Die NSA empfängt Aufträge von anderen Teilen der Regierung. Wenn also der oder die Außenministerin zu erfahren wünscht, was die deutschen Bundestagsabgeordneten so tun, dann macht sich die NSA daran, die Kommunikation des Deutschen Bundestages zu überwachen. Ebenso, wenn das Finanzministerium oder der Präsident diese Informationen wünscht. Im Großen und Ganzen arbeitet die NSA für andere Teile der Regierung. Sie hat Auftraggeber.*

Die eigentliche Frage lautet also: Sind Ihre Kommunikationsdaten von Interesse für jene Teile der US-Regierung, die befugt sind, eine Datenerfassung in Auftrag zu geben? Nun, ich vermute, dass zumindest einige Mitglieder des Deutschen Bundestages von der NSA überwacht werden. Ob gerade Sie überwacht werden bzw. eine Überwachung Ihrer Kommunikation beauftragt wurde, hängt davon ab, woran Sie arbeiten, mit welchen gesetzgebenden Bereichen Sie zu tun haben und, um es ganz offen zu sagen, wie

Original

to spy, or for the Israelis to spy, and your communications are just sitting out there and can be easily collected, then it probably won't be a lot of work for them to collect it. If your communications are better protected and you are a hard target, then maybe they'll have to decide, you know, Are you really that interesting?

But, to be perfectly frank, if the President says that he or she wants your communications, that they want to know what you're doing, if the NSA is not monitoring your communications, they're not doing their job. And I suspect that if they really want to get you, they will. The question is whether they'll be able to easily grab your telephone calls from the air, whether they'll be able to grab your unencrypted emails as they're going over international cables, or whether they will have to hack into your smartphone or send a laser through your bedroom window to listen to the conversations inside. But if they really want you, they'll get you.

Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank. - Dann kommen wir jetzt zu den Fragen von Frau Kollegin Renner. Auf der Liste stehen dann übrigens ferner Kollege von Marschall und Kollege Notz.

Martina Renner (DIE LINKE): Ich möchte ganz kurz die Frage von Herrn Edgar beantworten, wie wir es einschätzen, ob das Risiko, bei Spionage entdeckt zu werden, für die NSA nicht mittlerweile zu hoch ist in Deutschland und auch entsprechende diplomatische Verwicklungen nach sich zieht. Leider ist das nicht der Fall. Frau Stepanovich hat ja gesagt, es ist für die NSA legal, deutsche Parlamentarier und Parlamentarierinnen möglicherweise abzuhören. In Deutschland selbst nicht. Das ist hier ein Straftatbestand, geheimdienstliche Agententätigkeit. Die Frage „Warum wird er nicht verfolgt?“, die

Deutsche Übersetzung

gut oder schlecht Ihre persönlichen Sicherheitsmaßnahmen sind. Wenn Sie es den Amerikanern oder den Israelis leicht machen, Sie auszuspionieren, und Ihre Kommunikationsdaten einfach da draußen herumfliegen und problemlos erfasst werden können, dann kostet es die Geheimdienste wahrscheinlich keine große Mühe, sie zu erfassen. Wenn Ihre Kommunikationsdaten dagegen besser geschützt sind und Sie kein so leichtes Ziel abgeben, dann müssen die sich wahrscheinlich fragen, ob Sie wirklich so interessant sind.

Um jedoch ganz ehrlich zu sein: Wenn der Präsident bzw. die Präsidentin nach Ihren Kommunikationsdaten verlangt und wissen will, was Sie so tun, dann hätte die NSA ihren Job nicht erfüllt, wenn sie Sie nicht überwacht. Und ich vermute, dass sie Sie auch kriegen, wenn sie wirklich wollen. Die Frage ist, ob sie Ihre Telefongespräche einfach aus dem Funknetz abgreifen können, ob sie Ihre unverschlüsselten E-Mails einfach aus den internationalen Kabelverbindungen fischen können, oder ob sie sich in Ihr Smartphone einhacken oder Ihre Gespräche mit einem Laser durch Ihr Schlafzimmerfenster abhören müssen. Aber wenn sie es wirklich auf Sie abgesehen haben, dann kriegen die Sie auch.

Original

ist einfach zu beantworten: Die NSA hat einen Sonderstatus, sodass die Strafverfolgungsbehörden dort nicht agieren können, das Parlament nicht agieren kann - wir bekommen keine Unterlagen, Zutrittsrechte -, die Datenschutzbeauftragte nicht agieren kann, also keine Instanz in irgendeiner Form dort eine Revision oder eine Kontrolle ausüben kann. Das Einzige - -

Vorsitzender Dr. Patrick Sensburg: Das ist aber jetzt eine Einzelmeinung, nicht die Meinung des Ausschusses in Gänze.

Martina Renner (DIE LINKE): Na ja, aber die rechtliche - -

Vorsitzender Dr. Patrick Sensburg: Ich wollte es nur feststellen. Sie sind ja nicht als Sachverständige hier.

Martina Renner (DIE LINKE): Nein, aber Herr Edgar hatte das - -

Vorsitzender Dr. Patrick Sensburg: Es ist eine Meinung. *Eine* Meinung.

Martina Renner (DIE LINKE): Ja, das ist eine - meine - Meinung. Und das, was wir wissen zur Überwachungspraxis der NSA in Deutschland, ist tatsächlich im Wesentlichen aus den Snowden-Dokumenten für uns als Untersuchungsausschuss abgeleitet. Und deswegen ist er eben auch eine zentrale Person für unsere Beweisaufnahme. Er ist Zeuge hier im Untersuchungsausschuss. Und mich würde interessieren - weil das auch eine Frage ist, die wir derzeit an die Bundesregierung stellen und bisher nicht beantwortet bekommen haben; und da müsste ich einfach denjenigen bitten, zu antworten, der sich zuständig sieht - : Wie schätzen Sie die Strafvorwürfe gegen Edward Snowden ein?

Die Bundesregierung wird irgendwann beurteilen müssen, ob ihm politische Strafverfolgung in den USA droht und deswegen zum Beispiel in Deutschland Auslieferungsschutz bestehen könnte. Würden Sie anhand der Strafvorwürfe

Deutsche Übersetzung

Original

gegen Edward Snowden, auch vielleicht der Vorgeschichte, dem Entführungsversuch in Venezuela und Ähnlichem, so etwas bejahen wie, dass es auch die Möglichkeit gibt, dass man dies als politische Strafverfolgung qualifiziert, oder wie ist Ihre juristische Einschätzung? - Das wäre meine erste Frage.

Und die zweite ist dann wieder eine mehr technische, weniger juristische: Vom BND gelangen Daten an die NSA, und diese werden ja von dieser möglicherweise auch weitergegeben an andere Dienste, insbesondere der Five Eyes. Wie ist denn dann diese Situation rechtlich zu bewerten, wenn diese Informationen durch die NSA mit weiteren Diensten geteilt werden? Welche Unterschiede macht da die NSA, ob es sich dabei um Daten zu US-Bürgern, Europäern, Europäerinnen oder Daten von Bürgern und Bürgerinnen anderer Staaten handelt, also wenn diese Daten sozusagen noch mal an Dritte weitergegeben werden, was ja Praxis ist? Die arbeiten ja alle in Dateisystemen. Das würde uns auch noch mal insbesondere interessieren. - Danke.

Vorsitzender Dr. Patrick Sensburg: An wen war die zweite Frage?

Martina Renner (DIE LINKE): Das müsste ich einfach vielleicht ein bisschen offenlassen, wer sich mit dieser Frage „Weitergabe von Daten an Dritte durch die NSA“ beschäftigt hat. Da bitte ich einfach, dass Sie das untereinander abstimmen.

Vorsitzender Dr. Patrick Sensburg: Bei der ersten Frage ging es ja um rechtliche Sachverhalte, sowohl amerikanisches Recht als auch ein bisschen nationales Recht hier in Deutschland. Wären das Sie, Frau Gorski, die da zuerst berufen wäre? Sonst jemand anders. - Ja, die Juristen trifft es immer.

Martina Renner (DIE LINKE): Ich weiß, die Frage nach den Strafvorwürfen gegen Edward Snowden ist heikel; aber für uns ist sie zentral. Einfach noch mal als Erläuterung.

Deutsche Übersetzung

Original

Vorsitzender Dr. Patrick Sensburg: Ich will Ihnen jetzt nicht die Frage aufdrängen. Das wäre jetzt nur mein erster Eindruck. Vielleicht Sie, Frau Gorski, oder sonst jemand, der sich da berufen fühlt. Können Sie mir ein kurzes Zeichen geben? Sonst trifft es Frau Gorski.

Sachverständige Ashley Gorski: An ACLU attorney actually serves as a legal advisor to Edward Snowden. And as a result I think that it would not be prudent for us to comment on that question.

Vorsitzender Dr. Patrick Sensburg: Okay, schade. Denn das wäre ja vielleicht gerade interessant gewesen. - Möchte jemand anders dort einsteigen? - Okay, Herr Edgar.

Sachverständiger Timothy H. Edgar: So I guess I'll take this one. Just the facts here are, I think, fairly clear. Edward Snowden has been indicted in a federal court for stealing documents from the NSA and disclosing classified communications intelligence. My own personal opinion is that he is obviously guilty of these crimes, but the question of what do you do about that is a much more complicated one, because, as you know from my statement and from many of the things I've said here, there really is no doubt that without the Snowden disclosures we would not have this conversation about surveillance reform. And I believe that this conversation has not only improved the cyber-security, it's improved the way in which we protect personal information in law, and it's also, I would say, strengthened many of the NSA's surveillance programs themselves, for precisely the reasons that Mr. Soghoian said; you know, look at all these things the NSA continues to do. I think that's primarily the result of the fact that the public, both in the U.S. and in other countries as well, looked at many of those programs and said, Okay, we think there's some problems here that need to be corrected, but in general we do want the NSA to perform the valuable services it does for national security.

Deutsche Übersetzung

Sachverständige Ashley Gorski: *Edward Snowden wird durch einen Anwalt der American Civil Liberties Union rechtlich beraten. Von daher denke ich, es wäre nicht klug, wenn wir uns zu dieser Frage äußerten.*

Sachverständiger Timothy H. Edgar: *Dann übernehme ich wohl diese Frage. Die Fakten sind hier, denke ich, ziemlich klar. Edward Snowden wurde vor einem Bundesgericht angeklagt, Dokumente von der NSA gestohlen und vertrauliche Informationen der Fernmeldeaufklärung offenbart zu haben. Meiner persönlichen Meinung zufolge ist er dieser Straftaten ganz offensichtlich schuldig. Doch die Frage, wie man darauf reagiert, ist sehr viel komplizierter; denn es besteht, wie Sie meiner schriftlichen Stellungnahme und vielen meiner Aussagen hier entnehmen können, kein Zweifel daran, dass wir ohne die Snowden-Enthüllungen diese Gespräche über die Reform der Überwachung nicht führen würden. Und ich glaube, dass infolge dieser Gespräche nicht nur unsere Cybersicherheit verbessert wurde, sondern auch der gesetzliche Schutz unserer Privatdaten. Und ich würde sagen, dass auch viele der Überwachungsprogramme der NSA selbst dadurch gestärkt wurden, aus genau dem Grund, den Herr Soghoian nannte: Sehen Sie sich an, was die NSA alles weiterhin tut. Ich denke, das ist in erster Linie ein Ergebnis davon, dass die Öffentlichkeit sowohl in den USA als auch in anderen Staaten viele dieser Programme genauer betrachtet hat und gesagt hat: Okay, wir sind der Meinung,*

Original	*Deutsche Übersetzung*
	dass es hier einige Probleme gibt, die richtiggestellt werden müssen, aber ganz allgemein gesprochen möchten wir, dass die NSA weiterhin ihre wichtige Arbeit für die nationale Sicherheit leistet.
So all of those are positive outcomes of the Snowden revelations. So there have been several suggestions. One is status quo: he stays in Russia and continues to have a legal cloud over him, which makes it difficult for him to do things like travel and give testimony before this committee.	*All dies sind also positive Ergebnisse der Snowden-Enthüllungen. Es gab verschiedene Vorschläge, wie nun vorgegangen werden könnte. Zum einen die Fortsetzung des gegenwärtigen Zustands: Snowden bleibt in Russland und lebt weiter unter diesem juristischen Damoklesschwert, das es ihm erschwert, gewisse Dinge zu tun, wie beispielsweise zu reisen oder vor diesem Ausschuss auszusagen.*
He negotiates some kind of plea agreement with the United States government. That would be difficult in many cases to imagine happening from abroad. It would set a bad precedent for the U.S. government to be negotiating with someone outside its jurisdiction.	*Oder er handelt mit der US-Regierung irgendeine Art von Vergleich aus. Vom Ausland aus ist das in vielen Fällen schwer vorstellbar. Die US-Regierung würde einen ungünstigen Präzedenzfall schaffen, wenn sie mit einer Person außerhalb ihrer Gerichtsbarkeit verhandelt.*
And then many of Snowden's supporters have urged that he be pardoned for his offenses by the President, which is an unreviewable act of discretion by the President under our constitution and could be engaged in for any reason at all, including the possibility that it's just the best thing to do to put the whole issue behind us.	*Und schließlich haben viele Snowden-Unterstützer darauf gedrängt, dass er vom Präsidenten begnadigt wird. Das wäre ein von der Verfassung vorgesehener, rechtskräftiger Ermessensakt, der aus beliebigem Grund durchgeführt werden könnte, auch dem, dass es möglicherweise einfach das Beste wäre, die ganze Sache ad acta zu legen.*
So, those are possible outcomes for him himself.	*Das sind also mögliche Ergebnisse für Snowden selbst.*
I think your second question was on sharing arrangements. I'd be happy to take that as well. Essentially that goes back to the question that we were having earlier - the whole discussion, I think, we've been having about the Five Eyes and about other partners. And the question of "Do the protections of information that is shared from one government to another continue to follow?" would be worked out exactly in a sharing arrangement like that.	*Ich glaube, Ihre zweite Frage bezog sich auf das Teilen von Informationen. Darauf antworte ich ebenfalls gerne. Im Grunde führt das zurück zu der Frage, die wir vorhin besprochen haben, die ganze Diskussion zur Gruppe der Five Eyes und zu weiteren Partnern. Und die Frage, ob der Schutz von Daten, die von einer Regierung an eine andere weitergegeben werden, weiterhin gilt, würde genau in so einer Vereinbarung zur Informationsweitergabe ausgearbeitet werden.*
So certainly the United States would insist that partners treat U.S. person information the way	*Die Vereinigten Staaten würden also mit Sicherheit darauf bestehen, dass Partner die Daten von*

Original

that we would treat U.S. person information. And other countries have, in the past, insisted on reciprocal kinds of protections for their nationals. But this is a tricky area, and I would not necessarily assume that agreements universally contain those kinds of protections or that enforcement is always done. So I think that this is exactly the kind of compliance issue that needs to be addressed, and it's a particularly complex one because if you make the agreement too complex, you impede the very sharing that the agreement is supposed to allow. So it needs to be done in a way that allows the sharing to take place for the purpose that you signed the agreement in the first place, but where you aren't playing a game where, you know, I collect information and I give it to you, and you get to use it in ways that I couldn't use it. It's a basic principle, I think, of law, that you should not be able to do indirectly what you cannot do directly.

Deutsche Übersetzung

US-Personen genauso behandeln, wie wir die Daten von US-Personen behandeln. Und auch andere Staaten haben in der Vergangenheit auf beiderseitigem Schutz für ihre Staatsbürger bestanden. Doch dies ist ein sensibler Bereich, und ich würde nicht unbedingt davon ausgehen, dass Vereinbarungen immer diese Art von Schutz umfassen oder dass sie stets durchgesetzt werden. Ich denke daher, dass dies genau die Art von Compliance-Problemen ist, mit denen wir uns beschäftigen müssen. Und es ist ein besonders komplexes Problem, denn wenn die Vereinbarung zu kompliziert wird, beeinträchtigt man dadurch die Informationsweitergabe, die man eigentlich ermöglichen will. Man muss es also so lösen, dass die Informationsweitergabe genau für den Zweck erfolgen kann, für den man die Vereinbarung ursprünglich unterzeichnet hat, ohne das Spielchen zu spielen: Ich sammle Informationen und gebe sie an dich weiter, und du kannst sie so nutzen, wie ich es nicht durfte. - Es ist meiner Meinung nach ein grundlegendes Rechtsprinzip, sicherzustellen, dass man das, was man nicht direkt tun kann, auch nicht indirekt tun kann.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Wir kommen jetzt zu den Fragen des Kollegen von Marschall und dann des Kollegen von Notz.

Matern von Marschall (CDU/CSU): Vielen Dank, Herr Vorsitzender. - Ich möchte meine Frage anschließen an die Fragestellung von Kollegen Ströbele, weil ich von Dr. Halperin eigentlich die Frage, für mich jedenfalls, nicht hinreichend beantwortet sah, und würde deswegen in dem Fall jetzt zu Herrn Soghoian und Frau Stepanovich überleiten.

Wir erleben Sie ja als eine unglaublich engagierte Gruppe, zivilgesellschaftlich, rechtsstaatlich engagierte Gruppe. Ich weiß nicht genau, ob - um das noch mal zu vertiefen - das sozusagen repräsentativ ist für die amerikanische Öffentlichkeit, und zwar unabhängig von den politischen Lagern. Was ich aber glaube schon im-

Original

mer wieder wahrzunehmen, ist, dass es in Amerika ja eine traditionell verhältnismäßig große Skepsis gegenüber dem Staat gibt, also ein Engagement, was beide politische Lager eigentlich im Sinne des Liberalismus teilen, nämlich den Staat sich ein wenig fernzuhalten. Diese Skepsis teilen nach meinem Dafürhalten, vielleicht aus unterschiedlichen Erwägungen, beide großen politischen Lager.

Jetzt haben Sie, Herr Soghoian, uns vorhin angeraten, im Interesse unserer eigenen, na ja, sagen wir mal, Privatsphäre in unsere Sicherheit zu investieren. Sicherheit ist ja natürlich ein Begriff, der mindestens mal zwei Seiten hat. Wenn ich Sie richtig verstanden habe, dann ist ja die eben etwa in WhatsApp eingesetzte End-to-End-Verschlüsselungstechnologie so ausgestaltet, dass der Betreiber blind, wie Sie, glaube ich, gesagt haben, gegenüber der Kommunikation seiner Kunden ist. Es muss natürlich dann trotzdem die Frage auftauchen und vielleicht auch in der Gesellschaft auftauchen, auch unter denjenigen, die dann diese für sie sehr sichere Verschlüsselungstechnologie nutzen: Was bedeutet das denn eigentlich für diejenigen, die dem Staat Schaden zufügen wollen, also Terroristen etwa? Das heißt: Wie würden Sie auch unter dem Begriff der Sicherheit damit umgehen? Wie soll denn der Staat unter dem Eindruck, dass auch Terroristen diese Verschlüsselungstechnologie nutzen können, sich möglicherweise notwendigen Zugriff dann auf deren Kommunikation verschaffen?

Sie haben ja, glaube ich, vorhin gesagt, dass ohnehin das dann gar nicht genutzt würde, sondern dass die eigene Technologien vielleicht entwickeln oder dass - ich meine, das hat Herr Halperin angedeutet - dann Open-Source-Technologien genutzt würden. Aber wenn eben WhatsApp so sicher ist, dann würde ich als Terrorist doch einfach das auch nutzen und meine Kommunikation auf diesem Wege betreiben.

Deutsche Übersetzung

Original

Die Frage ist also: Macht sich die amerikanische Öffentlichkeit, die diese sichere, zunehmend sichere Verschlüsselungstechnologie nutzt, auch Gedanken darüber, wie der Staat im Interesse ihrer eigenen Sicherheit etwa vor den Angriffen von Terroristen einen Zugriff oder nicht dann auf diese Technologie haben sollte? Vielleicht können Sie beide einerseits mir erklären, ob das dann überhaupt möglich sein würde, Herr Soghoian, oder andererseits, Frau Stepanovich, mir erklären, wie man das in der Zivilgesellschaft diskutiert. - Danke sehr.

Sachverständiger Dr. Christopher Soghoian: Sure. I will attempt to answer all parts of your question. Let me first off say that this panel of experts is definitely not representative of the American society. The panel is five white people. America's a very diverse country ethnically, and if this panel represented all of America it would look very different.

Now with regard to, I think, the important question of encryption and "What do you do when both, good people and bad people use encryption?" That's a tough question. You are politicians and you get paid to make the tough decisions. As an advocate, I don't have to make a tough decision. I advocate for the views that I believe in, and I try to advocate the best arguments I can.

The fact is, there does not exist a form of encryption that will keep the most sophisticated intelligence services of foreign governments out, while allowing your domestic law enforcement agencies to get access to communications. If anyone tells you that it is possible to have your cake and eat it, too, they are lying. Or they are misguided. As politicians, you have to make a decision. You have to decide: What are you more afraid of, and what are you more interested in protecting? Do you wish to live in a society where your national police can monitor the communications of every

Deutsche Übersetzung

Sachverständiger Dr. Christopher Soghoian: *Gerne. Ich will versuchen, Ihre Frage in allen Teilen zu beantworten. Lassen Sie mich zuerst feststellen, dass diese Expertengruppe nicht repräsentativ für die amerikanische Gesellschaft ist. Es ist eine Gruppe von fünf Weißen. Die USA sind ein Land von großer ethnischer Vielfalt, und wenn diese Expertengruppe repräsentativ für die Gesamtgesellschaft der USA wäre, dann sähe sie ganz anders aus.*

Was nun die, wie ich denke, wichtige Frage nach der Verschlüsselung betrifft und danach, was man tun kann, wenn sowohl unbescholtene Bürger als auch Kriminelle Verschlüsselung einsetzen: Das ist eine schwierige Frage. Sie sind Politiker und werden dafür bezahlt, schwierige Entscheidungen zu treffen. Als Aktivist muss ich keine schwierigen Entscheidungen treffen. Ich vertrete die Standpunkte, von denen ich überzeugt bin, mit den besten mir zur Verfügung stehenden Argumenten.

Tatsache ist, dass keine Form der Verschlüsselung die am höchsten entwickelten ausländischen Nachrichtendienste aussperren und gleichzeitig den eigenen, innerstaatlichen Strafverfolgungsbehörden Zugriff auf Kommunikationsdaten erlauben kann. Wer behauptet, dass es möglich ist, beides gleichzeitig zu bekommen, lügt entweder oder sitzt einem Irrtum auf. Als Politiker müssen Sie entscheiden, was Ihnen mehr Sorge bereitet oder was Sie dringender schützen möchten. Möchten Sie in einer Gesell-

Original

potential target? Do you wish to live in a society where no communication is off limits to your police? Or do you wish to live in a society where your communications cannot be monitored by foreign governments? Because there's no way to have both.

Right now, in Germany, I suspect that many of your communications are being monitored, not just by my government but by many other hostile foreign governments who have not embraced the quasi-reforms that the U.S. has embraced. The only way to protect yourself from the meddling by foreign governments into your own political affairs, the only way to protect your domestic industries from espionage, from having your trade secrets stolen, is to use the strongest and most effective forms of communication encryption. But that will make life difficult for law enforcement.

Now, to be clear, encryption technology will not completely blind the state. Encryption makes life more difficult for the state. In many ways, surveillance is a question of economics. And right now the cost of spying is very low, and so what we see our well-resourced intelligence agencies doing is collecting everything they possibly can and trying to make sense of it. When you encrypt data, you raise the cost of surveillance, and it means that governments then have to turn to more effective but more personalized and targeted methods of surveillance, specifically the hacking of computers, the hacking of mobile devices, and other forms of intrusion upon the endpoints. You can make hacking more difficult, and with enough money and enough dedication you can make it extremely difficult for foreign governments to hack, but right now if you just encrypt that will make many, many forms of foreign intelligence collection difficult. They will probably still be able to

Deutsche Übersetzung

schaft leben, deren staatliche Polizei die Kommunikation jeder möglichen Zielperson überwachen kann? Möchten Sie in einer Gesellschaft leben, deren Polizei Zugriff auf jegliche Kommunikationsdaten hat? Oder möchten Sie in einer Gesellschaft leben, in der Kommunikationsverbindungen nicht von ausländischen Regierungen abgehört werden können? Denn beides gleichzeitig geht nicht.

Aktuell werden in Deutschland vermutlich viele Kommunikationsverbindungen überwacht, nicht nur durch meine Regierung, sondern auch durch die Regierungen zahlreicher feindlicher Staaten, die nicht die Quasi-Reformen in Angriff genommen haben, die die USA in Angriff genommen haben. Die einzige Möglichkeit, sich davor zu schützen, dass ausländische Regierungen sich in Ihre politischen Angelegenheiten einmischen, die einzige Möglichkeit, Ihre heimische Industrie vor Spionage und vor dem Diebstahl von Geschäftsgeheimnissen zu schützen, besteht darin, die leistungsfähigsten und wirksamsten Methoden zur Verschlüsselung Ihrer Kommunikationsdaten einzusetzen. Dadurch erschweren Sie jedoch die Arbeit der Strafverfolgungsbehörden.

Lassen Sie es mich ganz klar sagen: Verschlüsselungstechnologie wird die staatlichen Stellen nicht vollkommen blind machen. Sie macht die Arbeit der staatlichen Stellen schwieriger. Überwachung ist in vielerlei Hinsicht eine Frage der Wirtschaftlichkeit. Momentan ist Spionage nur mit sehr geringen Kosten verbunden, also erfassen unsere mit Ressourcen gut ausgestatteten Nachrichtendienste alles, was sie nur können, und versuchen es irgendwie auszuwerten. Wenn Sie Ihre Daten verschlüsseln, wird die Überwachung teurer, und das bedeutet, dass die Regierungen effektivere, aber auch stärker personalisierte und zielgerichtete Überwachungsmethoden einsetzen müssen, insbesondere das Einhacken in Computer oder Mobiltelefone oder andere Formen des Zugriffs auf Kommunikationsendpunkte. Sie können das Hacken erschweren, und mit genug Geld und Einsatz können Sie es ausländischen Regierungen extrem schwer ma-

Original

hack into the communications of your Chancellor, and they'll probably still be able to hack into your communications if you are really interesting, but they'll not be able to collect, you know, millions of communications taking place inside Germany.

You know, I think, whether we like it or not, we are moving at a very fast speed towards a world where governments - not just intelligence services but law enforcement agencies - will be hacking the computers of their own citizens and of foreign citizens. And I think that is a truly terrifying future. The idea that the police can hack into your webcam and enable the surreptitious collection of video footage from inside your bedroom, the idea that the police can remotely enable a microphone and capture audio recordings between a husband and wife or husband and husband, is something that I think should scare all of us, particularly as these capabilities are being deployed by law enforcement agencies without adequate debate by the democratically elected representatives who must make the tough decisions.

I personally think that the use of these advanced hacking and surveillance capabilities threaten democracy more than it benefits democracy from the ability to detect and thwart crimes. But if you decide as a parliament that you wish to give your own law enforcement agencies the appropriate power to hack, you know, that's up to you, but be very careful about that decision, because once you give these powers to your police, I think you'll be surprised how quickly they become used on a large scale.

Deutsche Übersetzung

chen, sich einzuhacken. Aber zum gegenwärtigen Zeitpunkt können Sie viele, viele Formen der Datenerfassung durch die Auslandsaufklärung anderer Staaten erschweren, indem Sie Ihre Daten einfach verschlüsseln. Die Auslandsgeheimdienste sind dann wahrscheinlich immer noch in der Lage, sich in den Computer der Bundeskanzlerin einzuhacken, und wahrscheinlich können sie sich auch noch in Ihre Kommunikationsverbindungen einhacken, wenn Sie eine Person von sehr großem Interesse sind, aber sie werden nicht mehr Millionen von Kommunikationsverbindungen innerhalb Deutschlands ausspionieren können.

Ich denke, ob es uns gefällt oder nicht: Wir bewegen uns mit großer Geschwindigkeit auf eine Welt zu, in der staatliche Einrichtungen - und zwar nicht nur Geheimdienste, sondern auch Strafverfolgungsbehörden - sich in die Computer ihrer Bürger und die ausländischer Bürger einhacken werden. Und das ist in meinen Augen eine wahrlich schreckliche Zukunft. Die Vorstellung, dass sich die Polizei in Ihre Webcam einhacken und heimlich Videobilder aus Ihrem Schlafzimmer aufzeichnen kann, die Vorstellung, dass die Polizei ferngesteuert Mikrofone aktivieren und Gespräche zwischen Ehemann und Ehefrau oder zwischen Ehemann und Ehemann aufzeichnen kann, diese Vorstellungen sollten uns allen Angst machen - besonders deshalb, weil diese Möglichkeiten von den Strafverfolgungsbehörden eingesetzt werden, ohne dass die demokratisch gewählten Volksvertreter, die die schwierigen Entscheidungen treffen müssen, dies angemessen diskutiert hätten.

Ich persönlich bin der Meinung, dass die Bedrohung der Demokratie durch den Einsatz dieser hoch entwickelten Hacking- und Überwachungsmöglichkeiten größer ist als der Vorteil, den die Demokratie gewinnt, wenn sie in der Lage ist, kriminelle Handlungen zu erkennen und zu verhindern. Wenn Sie als Volksvertretung entscheiden, dass Sie Ihren Strafverfolgungsbehörden die Macht geben möchten, sich [in Computer und Kommunikationsverbindungen] einzu-

Original

Deutsche Übersetzung

hacken, dann ist das Ihre Entscheidung. Sie sollten sie jedoch sehr sorgfältig treffen, denn wenn die Polizei erst einmal diese Möglichkeiten hat, dann werden Sie, so denke ich, überrascht sein, wie schnell diese Möglichkeiten im großen Rahmen eingesetzt werden.

Vorsitzender Dr. Patrick Sensburg: Okay. - Mrs. Stepanovich.

Sachverständige Amie Stepanovich: So what's often brought up in these conversations is the idea of privacy versus security, trade-offs and balancing. And while I think that those are insufficient frames of conversation for many reasons, several members of the U.S. Congress have gotten this right in saying that when you talk about whether or not to undermine encryption it is not a matter of privacy versus security, but security versus security.

Sachverständige Amie Stepanovich: *Das Abwägen oder der Kompromiss zwischen Datenschutz und Sicherheit ist ein Konzept, das in solchen Diskussionen oft zur Sprache kommt. Und obwohl ich der Meinung bin, dass dieser Referenzrahmen aus vielen Gründen unzureichend ist, haben viele US-Kongressabgeordnete recht, wenn sie sagen, dass es bei der Frage, ob man die Verschlüsselung einschränken soll oder nicht, nicht um Datenschutz versus Sicherheit geht, sondern um Sicherheit versus Sicherheit.*

Actually, the best way I've heard it described is that you cannot set up an encryption system that can only fail sometimes - which is what the FBI and several national states are asking for -, is a system that keeps everybody very secure, that protects your information from bad actors, that ensures that data breaches don't occur, but then in certain instances will fail in order to give law enforcement access to those communications. And that's simply not something that can be established, technologically speaking.

Die bisher beste Beschreibung der Situation, die ich gehört habe, lautet: Man kann ein Verschlüsselungssystem nicht so einrichten, dass es nur in bestimmten Fällen versagt. Und das ist es, wonach das FBI und mehrere Staaten verlangen: ein System, das alle gut schützt, das unsere Daten vor kriminellen Akteuren schützt, das Datenschutzverletzungen verhindert, aber das in gewünschten Fällen versagt, um den Strafverfolgungsbehörden Zugriff auf eben diese Kommunikationsdaten zu gewähren. Und so etwas lässt sich schon rein technisch gesehen gar nicht einrichten.

Technologist Matt Blaze from the United States, back in the 1990s when the U.S. was talking about mandating the installation of the Clipper chip in two pieces of technology in order to ensure U.S. government access to communications, showed how insecure that piece of technology really was. He is very fond of saying that cryptographers are not good at their jobs. And the reason he says that is not because he wants to berate himself as a cryptographer, but more because systems all have holes. It's very, very diffi-

Als die USA in den 1990er-Jahren überlegten, per Gesetz den Einbau des Clipper-Chips in zwei Technikkomponenten zu erzwingen, hat der US-amerikanische Technikexperte Matt Blaze demonstriert, wie unsicher dieser Chip tatsächlich war. Er sagt gerne, dass Kryptografen nicht besonders gute Arbeit leisten. Und er sagt das nicht, weil er seine eigene Arbeit als Kryptograf diskreditieren will, sondern um darauf hinzuweisen, dass alle Systeme lückenhaft sind. Es ist in unserem aktuellen System sehr, sehr schwer, Kommunikationsdaten zu schützen. Und sogar

Original

cult - in our current system - to protect communications. And that's why even in the San Bernardino case in the U.S. when the FBI was trying to break into the iPhone, which gained, I believe, international attention, and they went to the court and said that there is absolutely no way to get that information unless Apple built a new operating system to bypass the security measures - - The day before that case was supposed to go to hearing, they found a way in, because there are almost always vulnerabilities in technology, and we really need to be trying our hardest and devoting adequate resources - both money and time - to fixing those vulnerabilities to make ourselves more secure rather than trying to install more holes. Because, as I said in my spoken testimony, we cannot keep terrorists or criminals from using encryption.

So far, I think, the evidence that encryption has played any central role in attacks that we have seen so far is very, very weak. They possibly have used encryption but probably not in a way that was vital to the planning. For example, the San Bernardino attacks were basically planned over a kitchen table, and no backup encryption was going to be able to assist U.S. law enforcement in gaining access to communications that were happening within a home. Eventually, I would say, it is likely that we are going to see - probably soon - an attack where encryption did protect the information. I think that if we go on assuming that that's not going to be the case, we're arguing a short-term argument.

However, weakening encryption is probably not the answer. We do need to be talking about other ways that we can get information. I think we need to start engaging in an international conversation on government hacking, as Dr. Soghoian brought up. We have not done that so far; that was one of the reasons we published the

Deutsche Übersetzung

im Fall des San-Bernadino-Attentäters in den USA, der, so glaube ich, internationale Aufmerksamkeit erregt hat, als das FBI versuchte, das iPhone zu knacken, und vor Gericht ging und sagte, es bestünde keinerlei Möglichkeit, an die Daten heranzukommen, wenn Apple nicht ein neues Betriebssystem programmiert, mit dem sich die Sicherheitsvorkehrungen umgehen lassen - - Am Tag vor der Klageverhandlung haben sie es geschafft, ins System hineinzukommen, denn es gibt fast immer technologische Schwachstellen. Und wir müssen wirklich unser Möglichstes tun und ausreichende Ressourcen - sowohl Zeit als auch Geld - darin investieren, diese Schwachstellen zu beheben, um uns besser zu schützen. Und nicht versuchen, weitere Sicherheitslücken einzubauen. Denn wie ich bereits in meiner mündlichen Stellungnahmen sagte: Wir können Terroristen und Kriminelle nicht davon abhalten, Verschlüsselungslösungen einzusetzen.

Bisher, so denke ich, gibt es nur sehr, sehr schwache Belege dafür, dass Verschlüsselung bei den bisherigen Angriffen eine wichtige Rolle gespielt hätte. Wahrscheinlich wurde Verschlüsselung eingesetzt, aber wahrscheinlich nicht auf eine Weise, die für die Planung wesentlich war. So wurde der Terroranschlag von San Bernardino im Prinzip am Küchentisch geplant, und keine Backup-Verschlüsselung der Welt hätte den US-amerikanischen Strafverfolgungsbehörden dabei geholfen, Zugang zu Gesprächen zu erhalten, die im häuslichen Rahmen stattfanden. Ich denke, wir werden irgendwann - wahrscheinlich schon bald - einen Anschlag erleben, bei dem die Information durch Verschlüsselung geschützt wurde. Wenn wir weiterhin annehmen, dass dies nicht der Fall sein wird, denken wir meiner Ansicht nach zu kurzfristig.

Trotzdem ist die Schwächung von Verschlüsselung wahrscheinlich nicht die Lösung. Wir müssen über andere Möglichkeiten sprechen, diese Informationen zu erhalten. Ich denke, wir müssen uns auf internationaler Ebene über staatliches Hacking unterhalten, wie Dr. Soghoian ansprach. Das haben wir bisher nicht getan, und

Original

paper that we published earlier this week, to talk about what safeguards need to be in place. Because from Germany to Australia to the U.K. that is the practice that governments are engaging in, but we have very little information about what safeguards are in place to protect people. We need to talk about how metadata is made available and about how people get access to metadata and how often that plays a role in determining terrorist activity. I think there are a lot of things that we need to be bringing up about this conversation. I think weakening encryption is not only the easy answer but it's very much the wrong answer to this question.

Deutsche Übersetzung

das ist einer der Gründe, weshalb wir den Artikel geschrieben haben, der diese Woche erschienen ist: um ein Gespräch darüber anzuregen, welche Schutzmaßnahmen hier benötigt werden. Denn von Deutschland über Australien bis nach Großbritannien wird staatliches Hacking betrieben, aber wir haben nur sehr wenig Informationen darüber, welche Maßnahmen ergriffen werden, um die Menschen zu schützen. Wir müssen darüber sprechen, auf welche Weise Metadaten zur Verfügung gestellt werden und wie Menschen Zugang zu Metadaten erhalten und wie oft dies eine Rolle bei der Aufdeckung terroristischer Aktivitäten spielt. Ich denke, es gibt sehr viel, was wir in einer solchen Diskussion ansprechen müssen. Eine Schwächung der Verschlüsselung ist nicht nur die einfache, sondern in meinen Augen die völlig falsche Antwort auf diese Fragen.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich habe jetzt momentan nur noch zwei Wortmeldungen. Wenn es mehr würden, würde ich gleich mal fragen, ob wieder eine Pause notwendig ist. Aber wenn es nur noch zwei Wortmeldungen sind, dann würde ich vorschlagen, dass wir die erst mal versuchen. Das sind nämlich der Kollege von Notz und der Kollege Schipanski.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ich darf vielleicht eine ganz kurze Anmerkung machen zu der Frage, die der geschätzte Kollege von Marschall aufgeworfen hat, die uns ja tatsächlich bewegt. Ich würde mal etwas zugespitzt sagen: In Deutschland ist diese grundsätzliche Frage schon entschieden worden. Es gab ja viele Jahrzehnte zwei Deutschlands: ein Deutschland, in dem private Kommunikation massenhaft und anlasslos mitgelesen wurde, und eines, wo das nicht der Fall war und wo die „encryption" praktisch Artikel 10, also der Anspruch auf Privatsphäre, war. 1990 haben wir zum Glück den ersten Staat abgewickelt, weil wir es schändlich finden, wenn sozusagen anlasslos und massenhaft Privatsphäre ausgeschnüffelt wird. Deswegen glaube ich, dass wir jetzt nur noch einen Weg finden müssen, wie

Original

wir diese Grundrechte in das digitale Zeitalter übertragen. Dazu noch mal zwei Fragen.

Wir haben ja, ganz interessant, eigentlich sehr eigene Kooperationen mit der NSA untersucht nach 2001, „Eikonal“ und „Glotaic“ und solche Sachen, die sich gar nicht in den Snowden-Unterlagen fanden. Und es hat eben Zugriffe der NSA und amerikanischer Dienste auf die Glasfaser in Deutschland gegeben, eigene Zugriffe, wo die auch mitgemacht haben und teilweise die Technik gestellt haben usw. Da frage ich mich immer: Nach dem Freedom of Information Act und so: Gibt es eine Idee sozusagen, wie viele Arten solcher Kooperationen amerikanische Dienste weltweit machen? Das sage ich auch vor dem Hintergrund, Herr Soghoian, als wir das eben bewegt haben mit der Frage „Hat ‚data‘ eigentlich eine Flagge?“ Unsere Beispiele, die wir eben miteinander bewegt haben, funktionieren ja immer nur dann, wenn ich tatsächlich so ein braver Staatsbürger bin, dass ich meine 49- oder +1-Nummer auch immer mit ins Ausland nehme. Es wird Millionen von amerikanischen Staatsbürgern geben, die auf der Welt eben die Technik aus den Ländern nehmen und damit umgehen, in denen sie leben. Und wie erkennt man dann eigentlich ihre Nationalität und ihren Schutz, den sie eigentlich ja wohl verfassungsrechtlich in Anspruch nehmen könnten? Deswegen die Frage: Hat man eine Idee, wie viele Kooperationen es in dem Bereich gibt?

Meine zweite Frage - ich weiß nicht, vielleicht an Frau Gorski -: Wir haben uns sehr intensiv beschäftigt mit der Frage des Ringtausches - oder unter dem Stichwort diskutieren wir das -, nämlich sozusagen: Wenn man diese „American citizens/Non-American citizens“-Logik sozusagen mitnimmt: Wir haben genau das Gleiche, also unser Bundesnachrichtendienst. Für den gibt es Deutsche, das sind Grundrechtsträger, und es gibt Ausländer, und das ist der Afghane genauso wie der Österreicher, und die haben halt keine Grundrechte - Pech gehabt. Wenn kooperierende Geheimdienste dieser Logik folgen und Daten austauschen, teilweise eben auch automatisiert,

Deutsche Übersetzung

Original

läuft dann nicht eigentlich jedes Verfassungsrecht leer, also, ich sage jetzt mal, auch mal das der Amerikaner? Wenn eben britische, deutsche, französische Geheimdienste Daten über Amerikaner sammeln ohne Ende und wenn sie interessante Treffer haben oder Meldungen oder so, die dann austauschen, dann ist sozusagen der Umstand, dass die NSA sich irgendwie an die amerikanische Verfassung hält, schön, aber wertlos. Und deswegen die Frage, ob eben nicht, weil mir das eigentlich zu wenig rüberkommt, ob nicht die Universalität des Menschenrechts auf Privatsphäre eigentlich die Basis sein müsste und man eben aus dieser Nationallogik rauskommt, weil es am Ende des Tages in der digitalen Welt, im Internet Nationalstaatlichkeit in dem Sinne nicht gibt, vor allen Dingen wenn Geheimdienste eben kooperieren. - Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: An Mr. Soghoian und Frau Gorski, richtig?

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Da wäre mein Vorschlag, wer sich berufen fühlt.

Vorsitzender Dr. Patrick Sensburg: Mr. Soghoian.

Sachverständiger Dr. Christopher Soghoian: Okay, I'll take a stab at the parts of your questions that I think I can answer and then I'll pass the rest to my esteemed colleague.

We at the ACLU make extensive use of the Freedom of Information Act. And there are many great parts of FOIA, but it's not the superweapon of transparency that many people seem to think it is. We don't have a great track record when it comes to getting documents from the NSA. You know, I think - - There are many things where we don't even waste our time in filing a request with the NSA or the CIA because we know they're going to tell us to go away. So, I don't think it's possible to get that list of agreements between NSA and its foreign partners through FOIA. I don't know if anyone's tried, but I would be shocked if they would get anything

Deutsche Übersetzung

Sachverständiger Dr. Christopher Soghoian: *Okay, ich werde mir die Teile Ihrer Fragen vornehmen, die ich beantworten kann, und dann an meine geschätzten Kollegen weitergeben.*

Wir bei der ACLU nehmen den Freedom of Information Act oft und gerne in Anspruch. Der FOIA hat viele tolle Aspekte, aber er ist nicht die Wunderwaffe der Transparenz, für den ihn manche zu halten scheinen. Wir waren in der Vergangenheit nicht übermäßig erfolgreich darin, Unterlagen von der NSA zu erhalten. Wissen Sie, ich denke, es gibt viele Dinge, für die wir uns noch nicht einmal die Mühe machen, einen Antrag bei der NSA oder CIA einzureichen, weil wir schon wissen, dass sie uns doch nur fortschicken werden. Ich glaube also nicht, dass es möglich ist, diese Liste von Abkommen zwischen der NSA und ihren Auslandspartnern mit Hilfe des

Original

other than a "We can neither confirm nor deny" response.

On the question of international communications - - Ashley, why don't you follow up on their other thing?

Sachverständiger Timothy H. Edgar: I'm happy to assist my colleague. I guess thereare two questions: One is transparency about the countries beyond the Five Eyes that the NSA has agreements with. We have actually seen a fair amount of information leaked by Edward Snowden on these "third parties", as they're called. Just so you understand the lingo: the Five Eyes are "second parties", and so anyone else is a "third party," there is no such thing as a "first party" - that's you. So, I think that actually I would encourage Mr. Soghoian's and Ms. Gorski's organization to file that FOIA request, because I don't believe there has been a review of just how necessary it is to keep all of these agreements classified in 2016. Sometimes classification decisions continue indefinitely for reasons of bureaucracy, when they really no longer make any sense. It's well known that the NSA has relationships with a number of countries and to keep it secret, to me, seems like elevating secrecy over values that are more important without much gain to the national security.

Your second question was, "Well, look, if there's such extensive cooperation, not only among the Five Eyes, but in a broader set of countries, how can you really protect the rights of anyone? If everyone is a foreigner somewhere and the only rights that you extend are to your own nationals, then it would follow that you can just outsource

Deutsche Übersetzung

FOIA zu bekommen. Ich weiß nicht, ob es schon einmal jemand versucht hat, aber es würde mich schockieren, wenn die Antwort mehr gewesen wäre als „Das können wir weder bestätigen noch dementieren".

Was die Frage der internationalen Kommunikationsdaten betrifft - - Ashley, möchtest du auf das andere eingehen?

***Sachverständiger Timothy H. Edgar:** Gerne helfe ich meinem Kollegen hier aus. Ich denke, es gibt hier zwei Fragen. Zum einen die nach der Transparenz gegenüber Staaten außerhalb der Five-Eyes-Gruppe, mit denen die NSA Abkommen geschlossen hat. Edward Snowden hat tatsächlich ziemlich viele Informationen zu diesen sogenannten „dritten Parteien" offenbart. Um den Sprachgebrauch hier kurz zu klären: Die Five-Eyes-Staaten sind „zweite Parteien", daher sind alle anderen „dritte Parteien". Eine „erste Partei" gibt es in diesem Sinne nicht, das ist man selbst. Ich denke daher, dass ich der Organisation von Herrn Soghoian und Frau Gorski durchaus raten würde, die FOIA-Anfrage zu stellen, denn es wurde meines Wissens nicht überprüft, wie notwendig es ist, diese ganzen Abkommen im Jahr 2016 weiterhin als Verschlusssache zu behandeln. Manchmal läuft die Klassifizierung zur Verschlusssache aus bürokratischen Gründen unbefristet weiter, auch wenn sie nicht mehr wirklich sinnvoll ist. Es ist allgemein bekannt, dass die NSA Beziehungen zu einer Reihe von Staaten pflegt, und wenn man dies geheim hält, so schätzt man damit die Geheimhaltung höher ein als andere, wichtigere Werte, und das ohne bedeutenden Vorteil für die nationale Sicherheit.*

Ihre zweite Frage lautete: Wenn es eine derart umfassende Zusammenarbeit gibt, nicht nur zwischen den Five-Eyes-Staaten, sondern auch mit einer größeren Gruppe von Ländern, wie kann man dann überhaupt die Rechte irgendwelcher Bürger schützen? Wenn jeder irgendwo Ausländer ist und die Staaten nur ihren eigenen

Original

the surveillance of your nationals to somebody else." This is a classic problem in intelligence oversight which we call "reverse targeting", it is one example of that. And it really runs up against the legal principle that I mentioned earlier, which is certainly the principle that I saw being applied everywhere where I was in the intelligence community for six years, and that is that you may not indirectly do the thing that you are not allowed to do directly. So it would clearly be a violation for the NSA to ask the German BND, or any other partner, for information on a U.S. person, a U.S. citizen, that it could not gain itself directly because, for example, it had an order under the Foreign Intelligence Surveillance Act, or some other way of getting that information itself directly. And then the question is: Does the BND apply this principle? I don't know the answer to that question; I think it would be a good question for you to ask them.

Certainly the U.K., I believe, adopts a very similar principle when it comes to the Regulation of Investigatory Powers Acts, or RIPA, where they can't ask the NSA for information under Section 702 of FISA about a U.K. person, about a British citizen or national, without having a RIPA warrant under U.K. law. This fact, by the way, was only disclosed very recently in litigation, I think brought by Big Brother Watch, again in the Investigatory Powers Tribunal. And it was an important part of the decision about whether that relationship between the NSA and GCHQ, the British signals intelligence service, was lawful.

So that's sort of the complicated answer, and now I'm going to give you the basic answer, which is: it's important as a matter of human rights that we recognize the existence of the rights of privacy of everyone everywhere in the world. And, as a result, I think that requires that

Deutsche Übersetzung

Bürgern Rechte gewähren, dann folgt daraus, dass man die Überwachung der eigenen Bürger einfach an jemand anders outsourcen kann. Dies ist ein klassisches Problem bei der Kontrolle von Geheimdiensten, wir nennen es „Reverse Targeting", das ist ein Beispiel hierfür. Und es widerspricht wirklich dem Rechtsgrundsatz, den ich zuvor erwähnte und der in den sechs Jahren, in denen ich Teil der Nachrichtendienste war, überall befolgt wurde: Was direkt verboten ist, darf man auch nicht indirekt tun. Es wäre also eindeutig ein Verstoß, wenn die NSA den deutschen BND oder irgendeinen anderen Partner um Informationen über eine US-Person bitten würden, die sie nicht selbst direkt erfassen können, weil sie zum Beispiel nicht im Rahmen des Foreign Intelligence Surveillance Act dazu beauftragt sind und auch sonst keine Möglichkeit haben, die Informationen direkt zu bekommen. Die Frage ist dann: Folgt der BND diesem Rechtsgrundsatz? Das kann ich nicht beantworten. Ich denke, diese Frage müssen Sie dem BND stellen.

Großbritannien wendet, so glaube ich, auf jeden Fall in den Regulation of Investigatory Powers Acts, kurz RIPA, ein sehr ähnliches Grundprinzip an. Ohne RIPA-Befugnis unter britischem Recht dürfen britische Geheimdienste keine Informationen gemäß § 702 des FISA über britische Staatsangehörige oder Staatsbürger von der NSA einfordern. Dieser Sachverhalt wurde übrigens erst vor kurzem im Rahmen eines Gerichtsverfahrens offenbart, das, so glaube ich, von Big Brother Watch vor dem Investigatory Powers Tribunal angestrengt wurde. Und das hat bedeutend zu der Entscheidung über die Rechtmäßigkeit dieser Beziehung zwischen der NSA und der britischen Signalaufklärung GCHQ beigetragen.

Das war also sozusagen die komplizierte Antwort. Die grundsätzliche Antwort lautet: Es ist eine wichtige menschenrechtliche Angelegenheit, dass wir das Recht auf Privatsphäre jedes Menschen auf der Welt anerkennen. Und daraus ergibt sich meiner Meinung nach, dass alle ihre Maßstäbe anheben, wenn es darum geht, welche

Nur zur dienstlichen Verwendung

Original

all of our intelligence services raise their standards for what kinds of surveillance operations they conduct. So I think that principle is basic.

But I also think that - not just as a matter of realism but also as a matter of principle - it's perfectly reasonable for countries to adopt higher standards for surveillance of their own citizens. And they do so precisely for the example you gave of "the two Germanys."

The East German state was not a huge pioneer in surveillance and signals intelligence gathering on the entire world; it was a pioneer in mass surveillance of its own citizens for political control. Whereas the West German state has long cooperated with the NSA in engaging in signals intelligence collection directed against the Soviet threat and, today, against other threats.

So having rules that say, "Surveillance of our own citizens is a threat to our democratic system of a kind that's different from the kinds of surveillance operations - even mass surveillance operations - conducted around the world for legitimate purposes", I think is a reasonable thing to say. In other words, I think that if you apply - - To put it a different way: if the only protections that Americans had under law were PPD-28, that would be a huge disaster for our constitution, if the only protections that Germans had were some very minor rules about human rights protections that are extended to external surveillance operations of the BND, that would be a huge disaster, I think, for the German state. So I think you can have a higher bar for domestic surveillance. I think that you have to have a principle in intelligence sharing that you are not going to do indirectly what you cannot do directly, in other words, you're going to actually obey that principle yourself and, with all of your partners, you're going to make sure you don't circumvent those rules.

Deutsche Übersetzung

Art von Überwachungsoperationen sie durchführen. Ich denke, das ist ein grundlegendes Prinzip.

Ich denke jedoch auch - und zwar nicht aus realistischen, sondern aus prinzipiellen Gründen -, dass es absolut angemessen ist, wenn Staaten bei der Überwachung ihrer eigenen Bürger höhere Maßstäbe anlegen. Und das tun sie aus genau dem Grund, den Sie mit Ihrem Beispiel der zwei deutschen Staaten ansprachen.

Die DDR war kein großer Pionier, wenn es um die Überwachung und Signalaufklärung in der ganzen Welt ging. Sie war ein Pionier der massenhaften Überwachung ihrer eigenen Staatsbürger zum Zwecke der politischen Kontrolle. Die Bundesrepublik dagegen arbeitet seit langem mit der NSA zusammen und beteiligt sich an der Datenerfassung in der Signalaufklärung gegen die Bedrohung durch die Sowjetunion sowie - heute - durch andere Akteure.

Ich halte es daher für angemessen, wenn Staaten Regelungen einführen, die besagen, dass die Überwachung der eigenen Bürger die Demokratie auf andere Weise bedroht als Überwachungsoperationen - auch solche mit massenhafter Datenerfassung -, die zu rechtmäßigen Zwecken im Ausland durchgeführt werden. Anders gesagt: Wenn der einzige Rechtsschutz von US-Personen in der PPD-28 bestünde, wäre das eine Katastrophe für unsere Verfassung. Wenn der einzige Rechtsschutz der Deutschen einige untergeordnete Richtlinien zum Schutz der Menschenrechte wären, die auf externe Überwachungsprogramme des BND angewendet würden, dann wäre das, so denke ich, eine Katastrophe für Deutschland. Ich bin also der Meinung, dass für die Überwachung im Inland höhere Maßstäbe gelten dürfen. Ich denke, dass für die Informationsweitergabe der Rechtsgrundsatz gelten muss, dass man das, was direkt verboten ist, auch indirekt nicht tun darf. Anders gesagt: dass man dies Prinzip tatsächlich befolgen und gemeinsam mit allen Partnern dafür sorgen muss, dass niemand die Regeln umgeht.

Original

And then the final point is: there is a basic minimal level of protection under human rights principles that must apply to everyone around the world. And I think if you use all three of those principles, you've at least taken a small step towards trying to reconcile concerns about mass surveillance with a digital age.

Sachverständiger Dr. Christopher Soghoian: If I can just supplement my answer for one minute. So, it's true: we are all foreigners to every country but our own. But there is a big difference between the market for telecommunications products in the U.S. and the market for telecommunications products in most other countries. You use products made by American companies every day, and I don't use products made by German companies every day. I don't trust my data to a French email provider or my photographs to a Spanish hosting company. Most of my communications stay within the United States, whereas I suspect a significant number of your communications either go to a U.S. tech company or flow through a fiber-optic cable passing through my country. So, yes, we are all foreigners to everyone but ourselves, but some of us are foreigners more frequently than others. I think, you know, that goes for the rest of the world when it comes to using Gmail, but it also probably applies equally to many Europeans whose communications are passing through the Frankfurt Internet Exchange. And I suspect that the German government is probably taking advantage of that quite a bit. The sword really goes both ways there. And you would probably be wise to think about how much it makes sense to send your communications out of the country when they don't need to, and to what extent you should be entrusting your government's communications to foreign companies and to foreign-controlled telecom networks.

Deutsche Übersetzung

Und der letzte Punkt: Es gibt einen Mindestschutz im Rahmen der Menschenrechte, der für jeden Menschen auf der Welt gelten muss. Ich denke, wenn man alle diese drei Prinzipien anwendet, dann hat man zumindest einen kleinen Schritt getan, um die Bedenken bezüglich Massenüberwachung und das digitale Zeitalter miteinander zu versöhnen.

Sachverständiger Dr. Christopher Soghoian: *Ich würde meine Antwort hier gerne kurz ergänzen. Es stimmt: Im Ausland ist jeder von uns Ausländer. Es besteht jedoch ein riesiger Unterschied zwischen dem Markt für Telekommunikationsprodukte in den USA und dem Markt für Telekommunikationsprodukte in den meisten anderen Ländern. Sie nutzen tagtäglich Produkte und Dienste amerikanischer Unternehmen. Ich dagegen nutze nicht jeden Tag Produkte und Dienste von deutschen Firmen. Ich vertraue meine Daten nicht einem französischen E-Mail-Anbieter und meine Fotos nicht einem spanischen Hosting-Unternehmen an. Der Großteil meiner Kommunikationsdaten bleibt in den USA. Ich vermute jedoch, dass eine bedeutende Menge Ihrer Kommunikationsdaten entweder durch ein US-amerikanisches IT-Unternehmen oder durch ein Glasfaserkabel fließen, das in meinem Land verlegt ist. Daher stimme ich zu, dass jeder von uns irgendwo ein Ausländer ist, aber manche von uns sind häufiger Ausländer als andere. Ich denke, was die Nutzung von GMail angeht, trifft das auch auf den Rest der Welt zu. Aber ebenso betrifft es wahrscheinlich zahlreiche Europäer, deren Kommunikationsdaten über den DE-CIX laufen. Und ich kann mir vorstellen, dass die deutsche Regierung sich diese Tatsache ausgiebig zunutze macht. Es ist wirklich ein zweischneidiges Schwert. Und es wäre wahrscheinlich sehr klug von Ihnen, sich zu überlegen, wie sinnvoll es ist, Kommunikationsdaten ins Ausland zu schicken, wenn es nicht nötig ist, und inwieweit Sie Ihre staatlichen Kommunikationsdaten ausländischen Unternehmen und Telefonnetzen in ausländischer Hand anvertrauen möchten.*

Original	*Deutsche Übersetzung*
Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Hast du noch eine Nachfrage, Konstantin?	
Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Nein, ich habe noch eine Frage.	
Vorsitzender Dr. Patrick Sensburg: Ach so, ja, dann kommst du gleich dran. Ich habe nämlich jetzt noch drei Wortmeldungen. Du wärst dann wieder der vierte, wenn ich das richtig sehe. Kollege Schipanski, Kollege Flisek - wenn er wieder da ist bis dahin - und Kollegin Renner habe ich auf der Liste, und dann bist du wieder dran. - Die Frage ist jetzt einmal an das Panel: Brauchen Sie eine kurze Pause? Denn es gibt anscheinend doch noch für eine längere Zeit Fragen.	
Sachverständiger Dr. Christopher Soghoian: That would be nice.	***Sachverständiger Dr. Christopher Soghoian:*** *Das wäre schön.*
Vorsitzender Dr. Patrick Sensburg: Wie lange sollen wir machen? Jetzt mal eine halbe Stunde?	
Sachverständiger Dr. Christopher Soghoian: Five minutes is fine.	***Sachverständiger Dr. Christopher Soghoian:*** *Fünf Minuten ist prima.*
Vorsitzender Dr. Patrick Sensburg: Wollen Sie was essen oder nur einmal Luft schnappen?	
Sachverständiger Dr. Christopher Soghoian: Five minutes is fine. Five or ten minutes is enough.	***Sachverständiger Dr. Christopher Soghoian:*** *Fünf Minuten wären gut. Fünf oder zehn Minuten sind genug.*
Vorsitzender Dr. Patrick Sensburg: Dann machen wir 15 minutes.	
Sachverständiger Dr. Christopher Soghoian: Okay, sure.	***Sachverständiger Dr. Christopher Soghoian:*** *Okay, gerne.*
Vorsitzender Dr. Patrick Sensburg: I think that's fair then, 15 real minutes. Okay. - Die Ausschusssitzung ist dementsprechend 15 Minuten unterbrochen.	***Vorsitzender Dr. Patrick Sensburg:*** *Ich denke, das passt dann. 15 Minuten. Okay.*

Original

(Unterbrechung von
15.54 bis 16.13 Uhr)

Vorsitzender Dr. Patrick Sensburg: Meine Damen und Herren, die unterbrochene Sitzung des 1. Untersuchungsausschusses wird fortgesetzt. - Wir hatten aufgehört bei den Fragen des Kollegen Schipanski, der jetzt dran ist. Er kriegt auch das Rederecht, um seine Fragen zu stellen.

Tankred Schipanski (CDU/CSU): Vielen Dank, Herr Vorsitzender. - Ich knüpfe an die Fragen von Herrn Dr. von Notz an, die er gerade gestellt hatte. Die erste Frage geht an Herrn Dr. Halperin. Sie hatten diese Problematik des Ringtausches vorhin angedeutet oder in Ihrem Statement aufgeworfen. Das wurde jetzt bei uns übersetzt mit Outsourcing des Staatsbürgers oder Umdrehen der Zielerfassung. Es steht hier auch noch mal in unseren Unterlagen als „circular intelligence exchange“. Und der Sachverständige Edgar hat ja gefragt, ob wir das für den BND festgestellt haben. Das haben wir festgestellt, da fand kein Ringtausch statt. Jetzt hatten Sie das aber im Rahmen der NSA angesprochen. Von daher würde mich natürlich interessieren, ob Ihnen bekannt ist, ob über die NSA ein solcher Ringtausch stattfindet. - Das ist die erste Frage.

Die zweite Frage geht an den Sachverständigen Herrn Edgar. Er sprach - auch eben bei der Beantwortung der Frage von Herrn von Notz - die Problematik der ausländischen Bürger an und inwieweit die Privatsphäre des ausländischen Bürgers auch geschützt sein kann. Sie haben uns dann in Ihrem Eingangsstatement aufgezeigt, dass Sie sich da einen dreistufigen Prozess vorstellen können. Nun würde mich natürlich interessieren: Ist das eine persönliche Meinung von Ihnen, ein persönlicher Vorschlag, oder wird in den USA in der Tat nachgedacht, eine konkrete Regelung, einen konkreten Schutzmechanismus auch für ausländische Bürger einzurichten?

Vorsitzender Dr. Patrick Sensburg: Auch hier bezüglich des Ringtauschs ist es natürlich noch

Deutsche Übersetzung

Original

keine gefestigte Meinung des Untersuchungsausschusses oder gar Konsens. Auch das ist natürlich eine individuelle Bewertung.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Unbeachtliche Mindermeinung! - Heiterkeit)

- Wenn wir das jetzt durchzählen würden, wäre es kritisch. Ich frage jetzt nicht ab. - Okay.

Sachverständiger Dr. Morton H. Halperin: I don't know the answer to that question and I don't have any evidence on that. So I'm afraid I can't help you with that.

Sachverständiger Timothy H. Edgar: Thank you. - On the question of my proposal: it is just my personal view; it's my personal proposal. However, it was made as part of a round table discussion that a number of experts had last January, sponsored by the Hoover Institution, which is a think tank organization in the United States with a number of experts, who include foreign intelligence officials. My goal has been to inject a conversation about what kind of protections are owed to the rest of the world in a discussion about FISA Section 702, the Foreign Intelligence Surveillance Act, Section 702, next year, because I fear that the conversation may become a narrow one about the impact of that law on American citizens. And I actually think that that is not the main impact of Section 702 of the Foreign Intelligence Surveillance Act, precisely because I do think that the NSA, for the most part, obeys the rules that are given to it, either by Congress or the President. And in Section 702, the basic rule is: you can use this for someone reasonably believed to be a foreigner outside the United States. And we've had some discussion about how the NSA actually determines that and knows that. So it's been my goal, in next year, that we should have a broader conversation about privacy and about global privacy and not just about how particular programs by the NSA, whether it's this one or others, affect the privacy of Americans. Because I think, if we

Deutsche Übersetzung

Sachverständiger Dr. Morton H. Halperin: *Diese Frage kann ich nicht beantworten und habe auch keine Hinweise dazu. Ich fürchte also, dass ich Ihnen hier nicht helfen kann.*

Sachverständiger Timothy H. Edgar: *Vielen Dank. Was meinen Vorschlag betrifft, das ist nur meine persönliche Ansicht, mein persönlicher Vorschlag. Ich habe ihn allerdings im Rahmen von Gesprächen einer Expertengruppe am Runden Tisch im vergangenen Januar gemacht, die von der US-amerikanischem Denkfabrik Hoover Institution gefördert wurden und an denen auch ausländische Geheimdienstvertreter teilnahmen. Mein Ziel war es, im Rahmen der Gespräche zu § 702 des FISA im kommenden Jahr eine Diskussion darüber anzustoßen, welche Art von Schutz wir dem Rest der Welt schuldig sind. Ich fürchte nämlich, dass diese Gespräche sich auf die Auswirkungen dieses Gesetzes auf US-Personen beschränken könnten. Und ich bin auch der Ansicht, dass dies nicht die wichtigste Auswirkung von § 702 des Foreign Intelligence Surveillance Act ist, und zwar genau deshalb, weil ich glaube, dass sich die NSA größtenteils an die Regeln hält, die ihr auferlegt werden, sei es durch den Kongress oder den Präsidenten. Und die Grundregel von § 702 lautet: Dies ist anwendbar auf Personen, bei denen Grund zu der Annahme besteht, dass sie außerhalb der USA Ausländer sind. Wir haben ausführlich diskutiert, wie die NSA dies in der Praxis feststellen und wissen will. Mein Ziel war es daher, im kommenden Jahr ausführlicher über Datenschutz und Datenschutz auf weltweiter Ebene zu sprechen und nicht nur darüber, wie bestimmte Programme*

Original

do that, we kind of miss the opportunity that we have been given by the Snowden revelations.

One difference in the debate that I've noticed over the past three and a half years or so has been that we actually have had a conversation at all that goes beyond the protections we owe to American citizens. If you look at the kinds of reforms that were adopted in the 1970s when Dr. Halperin was spied on, they were all about protecting American citizens. And, today, we have a broader conversation.

So, the proposal I've made is just one way, one mechanism that Congress could use in order to narrow and beef up that provision of law in a way that would protect everyone who's a subject of it, rather than just focusing on how that information about U.S. persons might be shared.

Vorsitzender Dr. Patrick Sensburg: Okay, gut. - Dann kommt der Kollege Flisek als nächster Redner.

(Christian Flisek (SPD):
Ich mache es später!)

- Okay. - Dann hätte ich noch Frau Kollegin Renner auf der Liste. Weitere habe ich dann nicht auf der Liste. - Ich habe Kollegen von Notz vergessen, Entschuldigung.

Martina Renner (DIE LINKE): Wir sind bei der Aufklärung der Kooperation des Bundesnachrichtendienstes mit der NSA mit der Problematik konfrontiert, dass Grundlage dieser Zusammenarbeit in vielen Fällen sogenannte Memoranden sind, die wiederum unter Geheimhaltung liegen, also dem Parlament und den Kontrollgremien bis vor kurzem nicht bekannt waren, in Teilen bis heute nicht vollständig bekannt sind.

Deutsche Übersetzung

der NSA, sei es nun dieses oder andere, sich auf die Privatsphäre von Amerikanern auswirken. Denn wenn wir das täten, so würden wir, fürchte ich, die Chancen vertun, die uns die Snowden-Enthüllungen eröffnet haben.

Ein Unterschied in den Gesprächen, der mir im Laufe der vergangenen etwa dreieinhalb Jahre aufgefallen ist, war, dass wir überhaupt über Themen gesprochen haben, die über den Schutz, den wir US-Personen schulden, hinausgingen. Wenn Sie sich die Reformen ansehen, die wir damals in den 1970ern, als Dr. Halperin bespitzelt wurde, durchgesetzt haben, dann werden Sie feststellen, dass es dabei immer um den Schutz von US-Personen ging. Heute dagegen führen wir Gespräche auf breiterer Ebene.

Mein Vorschlag ist also nur eine Möglichkeit, ein Mechanismus, den der Kongress nutzen könnte, um diese gesetzliche Bestimmung so zu verschärfen und zu verstärken, dass sie alle schützt, die von ihr betroffen sind, und sich nicht nur auf die mögliche Weitergabe von Informationen über US-Personen konzentriert.

Original

Grundlage für diese Geheimhaltung sind wiederum Geheimschutzabkommen mit den USA, die wiederum dem Parlament nicht als Text vorlagen. Das ist eine etwas interessante Konstruktion.

Meine erste Frage zielt darauf, Herr Halperin vielleicht oder Herr Edgar - aber erst mal würde ich gerne Herrn Halperin ansprechen -: Ist das ähnlich in den USA? Werden dort auch Memoranden, die mit anderen Staaten - in dem Falle nicht als Regierung, sondern als Behördenchefs - konsultiert wurden, dem Parlament nicht vorgelegt? Oder kann man sich das als parlamentarische Kontrolleure in den USA gar nicht vorstellen, dass so etwas geheim bleibt?

Die zweite Frage, die in diesen Komplex gehört: Wir haben die Problematik, dass wir als Parlament in diesen bilateralen Abkommen als Dritte betrachtet werden, also bei uns greift die Third Party Rule. Würde man sich in den USA als Parlamentarier ebenfalls als dritte Partei bezeichnen, oder würde man einen originären eigenen Anspruch auf Einsichtnahme in diese Dokumente begründen?

Die zweite Frage geht an Herrn Soghoian. Ich glaube, es ist schon vorhin angesprochen worden: Bei den Operationen, die wir ganz faktisch untersuchen, gibt es eine zwischen der NSA und dem Bundesnachrichtendienst zum Abgriff von Kommunikationsdaten, insbesondere Internetverkehren, bei dem größten Telekommunikationsanbieter in Deutschland, der Deutschen Telekom, in Frankfurt. Und eine zweite, die wir untersuchen, ist interessanterweise zwischen dem Bundesnachrichtendienst und der CIA abgeschlossen worden, ebenfalls im Bereich SIGINT, also zur Massendatenerfassung, und zwar bei einem US-Anbieter, MCI WorldCom. Diesen Operationsnamen darf ich Ihnen nicht sagen, aber er beginnt mit G - L - O. Und wir rätseln bis heute, was möglicherweise Gegenstand dieser Operation sein könnte, weil ja auf diesem Provider auch US-amerikanische Verkehre liegen könnten. Könnte es eine Art Umgehung sein,

Deutsche Übersetzung

Original

dass man Dinge, die man nicht in den USA darf, dann in Europa versucht?

Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank. - Ich glaube, Mr. Halperin wäre jetzt der Erste gewesen, wenn ich es richtig verstanden habe, nicht?

Sachverständiger Dr. Morton H. Halperin: There is no such limit in the United States. The Congress appropriates the funds for the intelligence agencies in addition to the rest of the executive branch and can put whatever conditions it wants to on that funding. That doesn't mean that something was not shown to them that should have been. But there's no legal basis for denying them information.

Sachverständiger Timothy H. Edgar: I might actually disagree a little bit here with Dr. Halperin. There is certainly a legal basis in the form of executive privilege, which the government frequently uses to deny access to information to the Congress. However, Dr. Halperin is correct that oftentimes either that privilege is not invoked or waived, or it doesn't apply, or the Congress doesn't agree that documents are privileged. And it can use the weapon of an appropriations restriction and has done exactly that in the past. It has said, for example, Here is money that your agency can have, but it's not going to be available to you until you provide us with this document that you say is privileged.

When it comes to the specific questions about what kinds of documents are shared with oversight committees, I would say that there is usually a difference between the kinds of broad arrangements that might be encompassed in memoranda and the sort of very specific opera-

Deutsche Übersetzung

Sachverständiger Dr. Morton H. Halperin: *Eine solche Einschränkung gibt es in den Vereinigten Staaten nicht. Der Kongress weist den Nachrichtendiensten zusätzlich zu den übrigen Stellen der Exekutive Mittel zu und kann diese Mittelzuweisung mit beliebigen Auflagen verbinden. Das bedeutet nicht, dass dem Kongress eine Information vorenthalten wurde, die ihm hätte vorgelegt werden müssen. Sondern, dass keine rechtliche Grundlage besteht, dem Kongress Informationen vorzuenthalten.*

Sachverständiger Timothy H. Edgar: *Ich würde Dr. Halperin hier tatsächlich leicht widersprechen. Es gibt durchaus eine rechtliche Grundlage, nämlich das Executive Privilege [Vorrecht des Präsidenten, die Vorlage von Dokumenten vor Gericht abzulehnen], auf das sich die Regierung häufig beruft, um dem Kongress Zugang zu Informationen zu verwehren. Dr. Halperin hat jedoch insofern recht, als dieses Executive Privilege häufig nicht genutzt wird oder nicht anwendbar ist oder der Kongress nicht darin übereinstimmt, dass diese Unterlagen vertraulich sind. Er kann außerdem das Instrument der eingeschränkten Mittelzuweisung anwenden, was in der Vergangenheit auch getan wurde. So hat der Kongress beispielsweise gesagt: Hier sind die Mittel, die Ihre Agentur erhalten kann; aber sie stehen erst dann zur Verfügung, wenn Sie uns das Ihren Aussagen nach vertrauliche Dokument vorlegen.*

Was die genaueren Fragen zu der Art von Dokumenten angeht, die den Kontrollausschüssen vorgelegt werden, so würde ich sagen, dass es da normalerweise einen Unterschied gibt zwischen den umfassenden Bestimmungen, die möglicherweise in Memoranden enthalten sind, und den sehr spezifischen operationellen Einzelheiten.

Original

tional details. And I would say that the operational details would often not be shared, certainly not routinely and certainly not without adopting safeguards and accommodations. And it's the goal of both parties, usually, when there is a disagreement between the executive and the legislature, to resolve that disagreement as much as possible through cooperation. For example, perhaps the intelligence community doesn't want to share the documents directly with the committee, but would be willing to have staff review them at their offices. There are different ways of doing that.

So, what accommodations Germany comes to is, if course, a matter of its own constitutional law and its own separation of powers. It's obviously complex when you have a third party - in our case, I mean the United States - making its concerns known, because you're dealing with multiple entities here. Maybe the German government wants to share something and the U.S. government objects; or maybe the German government doesn't want to share something and the U.S. government thinks it's fine, but they don't want to tell you that because if they tell you that it undermines the position of their partners. So, all I can say is that as an oversight committee it would be my job - if I were advising you; if I were your lawyer - to press for as much access as you could get, to recognize that there may be legitimate confidentiality concerns on the part of the executive, and to try to work out an arrangement if that's at all possible.

Vorsitzender Dr. Patrick Sensburg: Okay. - Mr. Soghoian.

Sachverständiger Dr. Christopher Soghoian: I'm sorry, I don't have any particular knowledge of the cooperation between the BND and the CIA. So I can't help on that one.

Deutsche Übersetzung

Und ich würde sagen, dass die operationellen Einzelheiten oft nicht vorgelegt werden, ganz sicher nicht routinemäßig und sicherlich nicht, ohne dass Schutzmaßnahmen ergriffen wurden und ein Entgegenkommen stattfindet. Und bei Uneinigkeiten zwischen Exekutive und Legislative ist üblicherweise beiden Parteien daran gelegen, Konflikte so weit wie möglich gemeinsam zu lösen. Ein Beispiel hierfür wäre es, wenn die Geheimdienste die entsprechenden Dokumente nicht direkt an den Ausschuss weitergeben möchten, aber bereit sind, Mitarbeiter des Ausschusses in ihren Räumlichkeiten zu empfangen, damit diese die Dokumente vor Ort sichten können. Es gibt da verschiedene Möglichkeiten.

Welche Vereinbarungen Deutschland trifft, ist natürlich eine Frage des deutschen Verfassungs- und Staatsrechts und der Gewaltenteilung. Wenn noch eine dritte Partei - in unserem Fall sind das die USA - mit im Spiel ist und ihre Interessen geltend macht, wird es natürlich komplex, denn dann hat man es mit mehreren Instanzen zu tun. Vielleicht möchte die deutsche Regierung eine Information weitergegeben, doch die US-Regierung erhebt Einspruch. Oder die deutsche Regierung möchte eine Information nicht weitergeben, während die USA einverstanden sind, das aber nicht sagen möchten, um die Position ihrer Partner nicht zu schwächen. Ich kann also nur sagen, dass ich als Kontrollorgan die Aufgabe hätte - wenn ich Sie rechtlich beraten würde, wenn ich Ihr Anwalt wäre -, auf so viel Zugang zu Informationen zu drängen, wie Sie bekommen können, dabei anzuerkennen, dass die Exekutive möglicherweise berechtigte Einwände hinsichtlich der Vertraulichkeit hat, und gemeinsam zu einer Übereinkunft zu finden, soweit es irgendwie möglich ist.

Sachverständiger Dr. Christopher Soghoian: *Ich bedaure, ich weiß nichts Näheres über die Zusammenarbeit zwischen BND und CIA und kann Ihnen hier leider nicht weiterhelfen.*

Original

Vorsitzender Dr. Patrick Sensburg: Okay. - Dann wären wir jetzt bei den Fragen des Kollegen Flisek, und dann hätte ich noch Fragen. Weitere Redner habe ich derzeit nicht. - Kollege von Notz noch.

Christian Flisek (SPD): Ich habe noch eine Frage, und zwar würde ich die gerne an Herrn Dr. Soghoian stellen. Wir haben ja im Rahmen des Auftrags als Untersuchungsausschuss - ich hatte es schon erwähnt - im Endeffekt festzustellen: Was haben US-amerikanische und andere Dienste der Five-Eyes-Staaten im Zeitraum zwischen 2001 und 2013 in Bezug auf Deutschland getan? Wir haben naturgemäß natürlich da bestimmte Beweisschwierigkeiten, weil eben vonseiten der US-Administration und vonseiten der Intelligence Community in den USA beispielsweise hier keine Zeugen erscheinen und wir eben auch keine Akten beiziehen können. Wir haben uns aber jetzt schon vor längerer Zeit entschieden, dass wir die CEOs von einigen sehr prominenten US-amerikanischen Internet- und IT-Konzernen hier als Gesprächspartner einladen möchten.

Ich würde Sie gerne mal fragen auch in Bezug auf diese Phase unserer Arbeit: Wie würden Sie in dieser Zeitachse, beginnend 2001, die Zäsur 9/11, ich sage mal, eine Phase vielleicht auch eines überbordenden Patriotismus in den USA, der eben Konsequenzen hatte für die Frage „Wie eng arbeiten IT-, Internet-, Telefonfirmen auch mit Geheimdiensten zusammen - - Wie hat sich das im Laufe der Zeit bis zum heutigen Tage entwickelt, und wie würden Sie sozusagen die strategische Positionierung dieser Unternehmen auch in Bezug auf ihre weltweiten Geschäftsmodelle heute in der Phase nach Snowden einordnen, wo diese Thematik eine weltweite globale Öffentlichkeit bekommen hat durch Herrn Snowden und wo die Aufmerksamkeit auch dafür „Wie eng arbeiten solche Firmen im Zweifel mit US-Geheimdiensten zusammen?“ eine ganz andere Qualität erreicht hat? Also, ich würde Sie einfach mal bitten, vielleicht so, weil ich davon ausgehe, dass sich in dieser Zeitachse sehr viel geändert hat, wenn Sie das können, mir das mal

Deutsche Übersetzung

Original

darzustellen: Was sind nach Ihrer Einschätzung da die wesentlichen Etappen?

Sachverständiger Dr. Christopher Soghoian: That's a great question. I love that question, because it's the topic of my PhD dissertation. So thank you for asking that.

(Amusement)

As a general rule of thumb, the telephone companies are about as friendly to surveillance as it gets. It's not that it's changing. In the last two or three years, the major U.S. telecommunications companies, Verizon, AT&T, Sprint and T-Mobile, have embraced some degree of transparency, so they now all publish transparency reports revealing the number of requests that they get every year. And about a year ago, a year and a half ago, AT&T filed an amicus brief in a case that we brought regarding whether the government could get location data without a warrant. As far as I'm aware, that was the first time since 1928 that a U.S. phone company filed a pro-privacy brief in a court case; so that's pretty cool. But, as a general rule of thumb, the phone companies are extremely sympathetic to the needs of the intelligence community and of law enforcement.

I think there are a couple of reasons why this is the case. The first is the fact that the telephone companies were effectively an arm of the government, and at their creation they played a key role during World War I and World War II helping the NSA and its predecessor engage in surveillance.

The second factor is simply that the telecom companies are heavily regulated by the Federal Communications Commission, our telecom regulator, and the FCC actually uses its regulating power to enable surveillance. So, for example,

Deutsche Übersetzung

Sachverständiger Dr. Christopher Soghoian: *Das ist eine tolle Frage. Ich finde diese Frage super, denn das ist genau das Thema meiner Dissertation. Danke, dass Sie danach fragen.*

(Heiterkeit)

Als Faustregel lässt sich sagen: Die Telefongesellschaften sind so überwachungsfreundlich, wie man nur sein kann. Es ist nicht so, dass sich das ändern würde. In den vergangenen zwei bis drei Jahren haben die großen US-amerikanischen Telekommunikationsanbieter Verizon, AT&T, Sprint und T-Mobile ein gewisses Maß an Transparenz eingeführt. Sie alle veröffentlichen jetzt jährlich Transparenzberichte, in denen sie die Anzahl der erhaltenen Anfragen offenlegen. Vor etwa einem oder eineinhalb Jahren hat sich AT&T mit einem Amicus Curiae-Schriftsatz an einem von uns angestrengten Gerichtsverfahren beteiligt, in dem es darum ging, ob der Staat ohne Vollmacht Positionsdaten einholen darf. Meines Wissens war das seit 1928 das erste Mal, dass sich eine US-Telefongesellschaft in einem Gerichtsverfahren für die Seite des Datenschutzes eingesetzt hat; das ist also ziemlich klasse. Doch im Allgemeinen gilt die Faustregel, dass Telefongesellschaften den Ansprüchen der Nachrichtendienste und Strafverfolgungsbehörden gegenüber sehr aufgeschlossen sind.

Ich denke, es gibt hierfür zwei Gründe. Erstens waren die Telefongesellschaften früher im Endeffekt ein Staatsorgan und spielten nach ihrer Gründung eine wichtige Rolle im Ersten und Zweiten Weltkrieg, indem sie der NSA und ihren Vorgängerorganisationen bei der Überwachung halfen.

Zweitens unterliegen die Telefongesellschaften ganz einfach einer starken Regulierung durch die Federal Communications Commission, die unsere Kommunikationswege regelt. Und die FCC nutzt ihre regulierende Macht, um die Überwachung zu ermöglichen. Beispielsweise muss

Nur zur dienstlichen Verwendung

Original

before the FCC will grant an international telecommunications carrier permission to land a fiber-optic cable in the United States, that company has to sign a national security agreement with DHS and other parts of the U.S. national security community promising to provide law enforcement access to information, giving the U.S. government veto power over the installation of foreign-made telecommunications equipment in the network. If you do not do what the U.S. national security establishment wants, you do not get the license to land the cable. It's that simple. So the fact is that the FCC can make or break a telecom company's business. So who in their right mind would pick a fight with the U.S. government when the U.S. government can effectively kill your company?

In the tech sector you don't have that kind of regulation. Tech companies don't need permission from the U.S. government to exist in the way that the telecom companies are so dependent on permission because of the regulations that they operate under. And so the relationship between tech companies and the government has been very different. I think also there's very much a libertarian vein that runs through Silicon Valley, and many of the tech companies sort of follow that philosophy. To be clear: just because a Silicon Valley company believes that they should fight the government does not mean that they will not collect vast amounts of data for their own commercial business reasons; those are really seen as being two different things.

In terms of: what are the major milestones and how have things developed? A bulk NSA collection program was revealed under the presidency of George Bush, what was initially known as the "NSA warrantless wiretapping program."

Deutsche Übersetzung

ein internationaler Telekommunikationsnetzbetreiber, wenn er von der FCC die Genehmigung einholen möchte, ein Glasfaserseekabel in den USA verlegen zu lassen, eine Vereinbarung zur nationalen Sicherheit mit dem DHS [Department of Homeland Security] und anderen Organen der nationalen Sicherheit unterzeichnen. Hierin sichert er zu, Strafverfolgungsbehörden Zugang zu Kommunikationsdaten zu ermöglichen, und räumt der US-Regierung ein Vetorecht über die Installation von Telekommunikationskomponenten ausländischer Hersteller in seinem Netzwerk ein. Wenn man also nicht das tut, was die US-amerikanischen Geheimdienste von einem verlangen, dann bekommt man auch keine Verlegegenehmigung für das Kabel. So einfach ist das. Die FCC hat also die Macht, der Telefongesellschaft ihre Geschäftsgrundlage zu entziehen. Und welcher vernünftige Mensch würde sich mit der US-Regierung anlegen, wenn diese im Endeffekt sein Unternehmen ruinieren könnte?

Im Technologiesektor gibt es diese Art der Regulierung nicht. Anders als die Telekommunikationsanbieter, die aufgrund der Regulierung abhängig von Genehmigungen sind, benötigen Technologieunternehmen keine staatliche Existenzerlaubnis. Dadurch ist die Beziehung zwischen Technologieunternehmen und Regierung eine ganz andere. Außerdem ist das ganze Silicon Valley meiner Meinung nach von einer sehr liberalistischen Haltung geprägt, und viele Technologieunternehmen folgen dieser freiheitsliebenden Philosophie. Doch damit keine Missverständnisse entstehen: Ein Silicon-Valley-Unternehmen mag die Haltung vertreten, dass man sich gegen den Staat zur Wehr setzen sollte. Das bedeutet aber nicht, dass es nicht selbst Unmengen an Daten zu kommerziellen Zwecken sammelt. Beides betrachtet man als zwei ganz unterschiedliche Sachen.

Was die wichtigsten Meilensteine und die bisherige Entwicklung angeht: Es wurde bekannt, dass die NSA unter der Regierung vom George Bush massenhaft Daten gesammelt hat, in einem Programm, das ursprünglich als „NSA warrantless

Nur zur dienstlichen Verwendung

Original

When the major phone companies in the U.S. were sued for their participation, Verizon, one of our largest telecommunications companies, actually argued in court that they had a First Amendment free-speech right to share their customers' data with the NSA. I think that really goes to the philosophy of U.S. telecommunications companies, whereas the evolution of Silicon Valley companies, I think, is probably a little bit different. Many of them, I think, ignored cyber-security issues, they ignored the fact that governments could surveil their users for a long time. And then, I think, the Snowden disclosures put things on the front page and made life quite unpleasant. I think the fact is that rolling out cyber-security technologies costs money - you have to deploy engineers; sometimes you have to buy software or hardware -, and, I think, it was very easy for the engineers in the security teams at the companies, who wanted to deploy stronger encryption, who wanted to deploy stronger cyber-security protections - - it was difficult for them to get the attention from management and to get buy-in to divert resources from features that would win them customers to features that would be hidden from customers but that would improve security.

And, I think, what the Snowden disclosures did, because of the extreme embarrassment suffered by many U.S. tech companies, was: it opened the checkbooks within the security teams. And so, you know, after 2013, whatever the security team at Google wanted to do, they could do, as long as it did not interfere with the collection of user data for Google's business interests. But whatever the engineering team at Google wanted to do to protect the connection between Google and the customer, they were permitted and, in fact, encouraged to do. And so we've really seen,

Deutsche Übersetzung

wiretapping program" ["willkürliches Telefonüberwachungsprogramm der NSA"] bekannt wurde. Als die großen US-Telefongesellschaften wegen ihrer Beihilfe zu dieser Überwachung verklagt wurden, argumentierte Verizon, einer unserer größten Telekommunikationsanbieter der USA, vor Gericht, dass sie gemäß dem 1. Zusatzartikel der US-Verfassung, der das Recht auf freie Meinungsäußerung umfasst, das Recht haben, die Daten Ihrer Kunden an die NSA weiterzugeben. Ich denke, darin zeigt sich wirklich die grundlegende Haltung der US-Telefongesellschaften. Die Entwicklung der IT-Unternehmen im Silicon Valley sieht dagegen meiner Meinung etwas anders aus. Viele von ihnen haben Fragen der Cybersicherheit einfach ignoriert, sie haben die Tatsache, dass staatliche Stellen ihre Nutzer überwachen könnten, lange ignoriert. Ich denke, die Snowden-Enthüllungen brachten das Thema dann auf die Titelseiten, was bei den IT-Unternehmen für ziemliche Unannehmlichkeiten sorgte. Der Punkt war meiner Meinung nach, dass Technologien zum Schutz der Cybersicherheit teuer sind. Man muss Techniker einsetzen, man muss vielleicht Software und Hardware anschaffen. Und ich glaube, für die Techniker in den Sicherheitsteams, die gerne leistungsfähigere Verschlüsselungslösungen einsetzen und stärkere Cybersicherheitsvorkehrungen treffen wollten, war es nicht einfach, Gehör bei der Unternehmensführung zu finden und sie davon zu überzeugen, Ressourcen in Features zu stecken, die der Kunde nicht sieht, die aber die Sicherheit erhöhen, statt in solche, die zur unmittelbaren Kundengewinnung beitragen.

Und ich denke, die Snowden-Enthüllungen waren so peinlich für viele US-Unternehmen, dass sie nun bereit waren, Geld für die Sicherheit auszugeben. Und so kam es, dass nach 2013 alles, was das Sicherheitsteam bei Google machen wollte, gemacht werden konnte, solange dadurch nicht die Erfassung von Nutzerdaten für Googles wirtschaftliche Zwecke beeinträchtigt wurde. Alles, was das Technikerteam bei Google tun wollte, um die Verbindung zwischen Google und dem Kunden zu schützen, wurde dagegen gestattet und sogar aktiv gefördert. Was

Original

I think, a loosening of the corporate restrictions around the security teams in the companies, in that they're now empowered to roll out whatever encryption they want. The most recent, I think, development is the rise of companies like Apple and WhatsApp who see a competitive advantage in actually rolling out technologies that thwart surveillance of their customers by governments, and if not thwart, then at least make it somewhat difficult.

The last point I'll make is that while there are some companies that are positioning themselves as privacy leaders through the deployment of technology - such as Apple with its disk encryption, such as WhatsApp with its end-to-end messaging encryption -, there are other companies like Microsoft who have basically lagged as far behind as it is possible to lag in the deployment of security technologies, but have signaled to the marketplace that they care about privacy by engaging in litigation against the U.S. government. So Microsoft's litigation in the case involving data stored in Ireland was one case, and then, more recently, Microsoft is arguing that indefinite gag orders for law enforcement requests are unconstitutional. While I think it's great that Microsoft is engaging in litigation - and we've actually filed briefs in both of those cases that Microsoft has engaged in -, in many cases it would be even better if the company would hurry up and employ encryption. One of the Snowden disclosures revealed that Skype had actually weakened its encryption to make life easier for the FBI. Microsoft's Windows operating system encrypts data by default now, but with a key that is backed up to Microsoft servers so that Microsoft can turn over that key to government agencies that request it. It is extremely frustrating to see Microsoft doing so great in the legal arena against the U.S. government but doing so poorly in a technical arena when other companies are employing such basic industry standard protections at this point.

Deutsche Übersetzung

also wirklich geschah, so denke ich, war eine Auflösung der unternehmensinternen Einschränkungen der Sicherheitsteams, sodass diese jetzt in der Lage sind, jede Verschlüsselung einzuführen, die sie möchten. Die meiner Meinung nach jüngste Entwicklung ist der Aufstieg von Unternehmen wie Apple oder WhatsApp, die einen Wettbewerbsvorteil darin erkennen, Technologien einzusetzen, die die staatliche Überwachung ihrer Kunden verhindert oder zumindest erschwert.

Der letzte Punkt, den ich ausführen möchte, ist, dass es zwar Unternehmen gibt, die sich selbst als führend im Bereich Datenschutz positionieren, indem sie bestimmte Technologien einsetzen - so wie Apple es mit seiner Festplattenverschlüsselung macht und WhatsApp mit seiner Ende-zu-Ende-Verschlüsselung. Doch es gibt andere Unternehmen wie zum Beispiel Microsoft, die mit dem Einsatz von Sicherheitstechnologien so weit wie nur möglich hinterherhinken, aber durch ihre Klagen gegen die US-Regierung signalisieren, dass sie sich für Datenschutz einsetzen. In einer von Microsofts Klagen ging es um in Irland gespeicherte Daten. Und in einem neueren Fall argumentiert Microsoft, dass der unbefristete Maulkorb bezüglich Informationsanfragen von Strafverfolgungsbehörden verfassungswidrig ist. Ich finde es zwar großartig, dass Microsoft gegen die Regierung klagt - und wir haben übrigens auch Stellungnahmen in beiden Microsoft-Fällen abgegeben -, aber trotzdem denke ich, es wäre in vielen Fällen besser, wenn sich das Unternehmen mit dem Einsatz von Verschlüsselungslösungen etwas beeilen würde. Eine der Snowden-Enthüllungen legte offen, dass Skype seine Verschlüsselung sogar geschwächt hatte, um dem FBI die Arbeit zu erleichtern. Microsofts Betriebssystem Windows verschlüsselt jetzt standardmäßig, aber das mit einem Schlüssel, der auf Microsoft-Servern gespeichert wird, sodass Microsoft ihn auf Anforderung an staatliche Behörden aushändigen kann. Es ist extrem frustrierend, zu beobachten, dass Microsoft sich auf gerichtlicher Ebene so gut gegen die US-Regierung wehrt und auf der technischen Ebene so wenig

Original

Vorsitzender Dr. Patrick Sensburg: Okay. - Jetzt habe ich zuerst Kollegen von Notz. Dann komme ich.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. - Ich wollte auch wieder eine eher technische Frage noch mal ansprechen, auf die wir gestoßen sind im Rahmen der Ermittlungen, die wir hier durchgeführt haben, nämlich die sogenannte Selektorenproblematik, gerade weil vorhin die Zahl angesprochen wurde, wie viele US-Citizens irgendwie auf dem Schirm sind. Wenn ich die Zahl richtig verstanden habe, sind es circa 90 000, 93 000. Wir haben ja gelernt, dass in der Kooperation zwischen BND und NSA der Bundesnachrichtendienst für die NSA eine zweistellige Millionensumme an Selektoren gesteuert hat. Und Selektoren können sein - das wissen Sie wahrscheinlich, nicht? - IMEI-Adressen, Handynummern, E-Mail-Adressen, Schlagworte, ganz viele unterschiedliche Dinge. Da würde mich mal interessieren, ob es im Hinblick auf die rechtlichen Voraussetzungen in den USA ein Prozedere gibt, was man eigentlich steuern darf, und wer diese Selektoren, mit denen man dann in den großen Datenmengen rumfischt, eigentlich freigibt und wer die Frage stellt: „Ist das“ - ich sage mal - „die IMEI-Nummer von Michelle Obama oder vielleicht von Osama bin Laden?“ Also, gibt es da ein Controlling, auch in zeitlicher Hinsicht? Es kann ja sein, dass man einen bestimmten Selektor in einer bestimmten Zeit steuert; aber dann erledigt sich irgendwie wieder das Ziel und so. Und deswegen fragen wir uns eben bei dieser großen Anzahl von Selektoren, wie eigentlich die rechtlichen Voraussetzungen dafür sind, dass solche Selektoren gesteuert werden, um damit den Datenstrom oder die „metadata“, die man angehäuft hat, eben zu durchfischen.

Vorsitzender Dr. Patrick Sensburg: An wen geht die Frage?

Deutsche Übersetzung

tut, während andere Unternehmen diese grundlegenden Standardschutzmaßnahmen längst eingeführt haben.

Original	*Deutsche Übersetzung*
Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Sie geht an Frau Gorski.	
Sachverständige Ashley Gorski: I can begin, and I believe Mr. Edgar may be interested in jumping in as well. Is that okay, to have two responses?	***Sachverständige Ashley Gorski:*** *Ich kann gerne anfangen und glaube, dass Herr Edgar ebenfalls etwas dazu zu sagen hat. Ist es in Ordnung, wenn wir beide antworten?*
So, just to clarify: that 93,000 number relates to the number of targets, not targeted accounts, which may be greater, but the number of targets under Section 702 of FISA. And in order to be a target under Section 702 of FISA, you need to be a non-U.S. person reasonably believed to be located abroad. So just to clarify: the 93,000 number does not correspond to U.S. citizen targets.	*Zur Klärung: Die Zahl 93 000 bezieht sich auf die Zielpersonen, nicht die Anzahl der Zielkonten, welche höher liegen kann, sondern auf die Anzahl der Zielpersonen gemäß § 702 des FISA. Um als Zielperson gemäß § 702 des FISA infrage zu kommen, muss man eine Nicht-US-Person sein, bei der Grund zu der Annahme besteht, dass sie sich im Ausland aufhält. Nur um das klarzustellen: Bei den 93 000 handelt es sich nicht um US-Zielpersonen.*
Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Aber da lassen Sie mich nachfragen. Das heißt, diese 93 000 sind Nicht-US-Citizens? Und wie kann es dann sein, dass der Bundesnach- -	
Sachverständige Ashley Gorski: They are non-U.S. persons, so they are individuals who are reasonably believed to be located abroad.	***Sachverständige Ashley Gorski:*** *Sie sind Nicht-US-Zielpersonen, also Personen, von denen man davon ausgeht, dass sie im Ausland sind.*
Sachverständiger Timothy H. Edgar: Right, it's actually broader - - Sorry. It's actually broader than non-U.S. citizens. It includes - - Legal permanent residents could also not be targeted under that. So, those 93,000 are all foreigners. But only under one part of the NSA's authority, which is the FISA Section 702 authority; that's for collection inside the United States.	***Sachverständiger Timothy H. Edgar:*** *Richtig, es ist tatsächlich weiter gefasst - - Verzeihung. Das umfasst eigentlich mehr als nur Nicht-US-Bürger. Es umfasst auch - - Personen mit dauerhaftem rechtmäßigem Aufenthalt könnten also nicht abgehört werden. Also sind diese 93 000 alle Ausländer, aber nur gemäß einem Teil der NSA-Befugnis, nämlich der Befugnis zur Erfassung von Daten innerhalb der Vereinigten Staaten gemäß § 702 des FISA.*
For collection outside the United States - and I think this is important to understand - there really is no control about selectors or targets. The thing that comes closest to that is the restrictions on bulk collection in PPD-28, and those do not apply at the collection stage but at the use stage. Essentially, what they say is: if	*Was die Datenerfassung außerhalb der Vereinigten Staaten betrifft - und das ist meiner Meinung nach ein wichtiger Punkt -, gibt es keine wirkliche Kontrolle bezüglich Selektoren und Zielen. Was dem am nächsten käme, ist die Beschränkung von massenhafter Datenerfassung durch die PPD-28, und die bezieht sich nicht auf die*

Original

you are not using selectors - in other words: you're just grabbing huge quantities of data without filtering them with selectors -, then there are certain restrictions that apply; you can only use it for certain purposes. But the concept of selectors is really a concept that applies in Section 702 collection. It also restricts the ability of the NSA to use selectors associated with U.S. persons. But when it comes to non-U.S. persons, there's no restriction. And in terms of the numbers: we really don't know the number of selectors in total that the NSA is using. It's probably a very, very large number of selectors that is being used in EO 12333 collection. And so, those numbers that you suggested certainly aren't surprising.

And it's more a question not of authority, of legal authority, because the NSA has broad authority to collect data outside the United States that it doesn't believe involve U.S. persons, it's really a question of the technical mechanisms used to acquire the data. So it doesn't make sense to acquire data in bulk if you can acquire it in a more targeted way and have the same impact. So, this is just a good example of how our debate - Dr. Soghoian and I were just discussing this - hasn't really covered the full panoply of the NSA activities - that's what I've wanted to have a bigger debate about -, it's really focused more on specific programs that Snowden disclosed, particularly ones that seemed to have an impact on American citizens.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Wenn ich ganz kurz noch einmal nachhaken darf. Das leuchtet mir ein; aber es wirft doch Fragen auf. Also, wir haben einmal die Problematik, dass wir häufig Filter eben gar nicht richtig einstellen können - so haben wir das zumindest von unserem Nachrichtendienst gelernt, der auch mit viel US-Technik arbeitet -,

Deutsche Übersetzung

Datenerfassung selbst, sondern auf die Nutzung. Im Wesentlichen heißt es dort, dass bestimmte Einschränkungen gelten, wenn man keine Selektoren verwendet, also im Grunde nur Riesenmengen an Daten abgreift, ohne sie anhand von Selektoren zu filtern. Man kann diese Daten nur für bestimmte Zwecke nutzen. Aber richtig zum Tragen kommt das Konzept der Selektoren bei der Datenerfassung gemäß § 702. Der § 702 schränkt auch die Möglichkeiten der NSA ein, Selektoren in Verbindung mit US-Personen anzuwenden. Bei Ausländern dagegen gibt es keine Einschränkung. Und was die Zahlen betrifft, so wissen wir wirklich nicht, wie viele Selektoren die NSA insgesamt einsetzt. Wahrscheinlich wird eine sehr, sehr große Zahl an Selektoren in der Datenerfassung nach EO 12333 eingesetzt. Daher sind die von Ihnen genannten Zahlen nicht überraschend.

Und es ist weniger eine Frage der rechtlichen Befugnis, denn die NSA hat weitreichende Befugnisse, außerhalb der USA Daten zu erfassen, die ihrer Ansicht nach keine US-Personen betreffen, sondern eine Frage der technischen Mechanismen, die bei der Datenerfassung zum Einsatz kommen. Es ist also nicht sinnvoll, massenhaft Daten zu erfassen, wenn eine gezielte Datenerfassung dieselbe Wirkung hätte. Das ist ein gutes Beispiel dafür, dass unsere Debatte nicht das gesamte Spektrum der NSA-Aktivitäten abdeckt; darüber habe ich mich auch gerade mit Dr. Soghoian unterhalten. Ich würde gerne eine umfassendere Debatte darüber führen. Diese Debatte bezieht sich eher auf bestimmte Programme, die im Rahmen der Snowden-Enthüllungen bekannt gemacht wurden, besonders solche, die einen Einfluss auf amerikanische Staatsbürger zu haben schienen.

Original

dass man eben bestimmte Leute gar nicht ausfiltern kann. Und, ich meine, natürlich gibt es US-internen Kommunikationsverkehr; aber US-Citizens kommunizieren ja über den ganzen Planeten, jeden Tag milliardenfach. Und der „pillow talk“ usw. der ganzen Soldatinnen und Soldaten, die im Ausland stationiert sind, all das läuft ja über die internationalen Netze. Deswegen also noch mal die Frage: Gibt es kein Bedürfnis von parlamentarischer Kontrollseite aus, irgendwie zu verstehen, wer da was einsteuert? Denn mir scheint natürlich der Missbrauch oder die Fehleranfälligkeit gigantomanisch zu sein. Und diese 13 Millionen Selektoren, von denen wir ungefähr ausgehen, sind tatsächlich wahrscheinlich nur ein bestimmter Bereich; wahrscheinlich sind es viel, viel mehr. Und da wird ja eben nicht nur nach Nationalitäten, sondern da wird auch nach Schlagworten gesucht usw.; also da müssen jeden Tag viele, viele Amerikaner betroffen sein. Deswegen frage ich mich, ob es nicht doch irgendwie eine Form der Kontrolle geben müsste nach Ihrer Auffassung oder wie man das machen könnte.

Sachverständiger Timothy H. Edgar: Well, I certainly wish to - - Just to go directly to your question of who picks the selectors. The answer is: basically intelligence analysts who would as part of their work pick these kinds of selectors, either in the BND or in the NSA or in any other service. If it’s controlled by a law, such as Section 702 of FISA, there are procedures that are required to be followed. If it’s Executive Order 12333, there are less strict procedures, but procedures to protect the interests of U.S. persons that maybe have their communications intercepted. Those are the U.S. person procedures - as they’re sometimes called -, or United States Signals Intelligence Directive 18, USSID 18, which applies to those.

So it may not give you much comfort that an intelligence analyst can decide on a selector based essentially on the intelligence requirements given to that agency to collect intelligence. If it’s

Deutsche Übersetzung

Sachverständiger Timothy H. Edgar: *Nun ich würde gerne - - Um direkt auf die Frage einzugehen, wer die Selektoren auswählt. Die Antwort lautet: Das machen im Grunde Analysten des BND oder der NSA oder eines anderen Geheimdienstes, zu deren Aufgaben es gehört, diese Art Selektoren auszuwählen. Wenn dies durch ein Gesetz kontrolliert wird, wie beispielsweise durch § 702 des FISA, dann gibt es Verfahren, die dabei befolgt werden müssen. Wenn die Kontrolle nach EO 12333 erfolgt, gibt es weniger strenge Verfahrensvorgaben; aber es gibt Verfahren zum Schutz der Interessen von US-Personen, deren Kommunikationsdaten möglicherweise abgefangen werden. Das sind die Verfahren zu US-Personen, wie sie manchmal genannt werden, oder die United States Signals Intelligence Directive 18, USSID 18, die hier gelten.*

Es wird Sie also wahrscheinlich nicht besonders beruhigen, dass Geheimdienstanalysten über Selektoren entscheiden und diese Entscheidung im

Original

not controlled by law in the way that I've described, either for a U.S. person or for collections occurring in the U.S., there's general oversight. The oversight by U.S. Congress of this, I think it's fair to characterize it as relatively lax. They certainly do have the authority to conduct oversight of EO 12333 activities, but they have tended to focus more on those activities controlled by the Foreign Intelligence Surveillance Act. So, part of what I'm trying to do in my proposal is to make some of these kinds of decisions more subject, more transparent, and more available to some kind of legal control.

Sachverständiger Dr. Christopher Soghoian: You asked also about surveillance of U.S. troops by the NSA. There was a scandal just a few years ago revealing that NSA analysts were monitoring the telephone sex calls between troops and their spouses back home. And not only were they listening to these calls, but then analysts would actually share with each other their favorite clips from these extremely intimate, private telephone calls that had nothing to do with terrorism, nothing to do with legitimate needs to monitor calls. And so, certainly the conversations of U.S. troops have been caught up not only in the dragnet but then in the subsequent monitoring systems that use data that's been collected.

Sachverständige Ashley Gorski: And just one final point. Senator Dianne Feinstein, the former chairman of the Senate Intelligence Committee, has been very clear that the Senate Intelligence Committee has been unable to sufficiently oversee EO 12333 surveillance and the sprawling surveillance programs under that authority.

Deutsche Übersetzung

Wesentlichen auf den Informationsanforderungen beruht, nach denen der Geheimdienst Daten erfasst. Wenn das nicht, wie eben beschrieben, gesetzlich kontrolliert ist, weder in Bezug auf US-Personen, noch für Datenerfassungsprogramme innerhalb der USA, dann gibt es eine allgemeine Kontrolle. Die Kontrolle durch den US-Kongress in diesem Bereich lässt sich meiner Meinung nach als relativ nachlässig bezeichnen. Der Kongress hat zwar die Befugnis, die Aktivitäten nach EO 12333 zu kontrollieren, aber sie haben sich in der Vergangenheit eher auf die Aktivitäten konzentriert, die durch den Foreign Intelligence Surveillance Act kontrolliert werden. Meine Absicht in meinem Vorschlag ist es daher unter anderem, diese Art Entscheidungen stärker zum Gegenstand gesetzlicher Kontrollen zu machen, sie transparenter und besser greifbar für gesetzliche Kontrollen zu machen.

Sachverständiger Dr. Christopher Soghoian: *Sie fragten auch nach der Überwachung von US-Truppenangehörigen durch die NSA. Vor einigen Jahren gab es einen Skandal, als bekannt wurde, dass Analysten der NSA Sextelefonate von Truppenangehörigen mit ihren Partnern in der Heimat überwachten. Und zwar hörten die Analysten diese Telefonate nicht nur mit, sondern tauschten auch untereinander ihre Lieblingsmitschnitte dieser extrem intimen und privaten Telefongespräche aus, die nichts mit Terrorismus zu tun hatten und nichts mit irgendwelchen rechtmäßigen Gründen, Telefonate zu überwachen. Also sind die Gespräche von US-Truppenangehörigen nicht nur mit ins Netz der Datenerfassung gegangen, sondern auch in den anschließenden Überwachungssystemen gelandet, die die erfassten Daten auswerten.*

Sachverständige Ashley Gorski: *Und noch eine letzte Sache: Senatorin Dianne Feinstein, die ehemalige Vorsitzende des Senate Intelligence Committee, hat ganz klar gesagt, dass das Senate Intelligence Committee nicht in der Lage war, die Überwachung nach EO 12333 und die ausufernden Überwachungsprogramme, die im Rahmen dieser Befugnis durchgeführt wurden, ausreichend zu kontrollieren.*

Original

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Mit Frau Feinstein hätten wir übrigens auch gerne gesprochen - aber das ging terminlich irgendwie bei ihr nicht -, als wir in Washington waren.

Ich hätte zwei Fragen. Die erste Frage vielleicht noch mal an Herrn Edgar. Mich hat jetzt so ein bisschen die Frage vom Kollegen von Notz angeregt, noch mal etwas grundsätzlicher nach den Selektoren zu fragen. Und, Herr Soghoian, vielleicht können Sie dann auch reinspringen; die zweite Frage wird dann nämlich sowieso an Sie gehen.

Mich interessiert ein bisschen, wie das mit den amerikanischen Selektoren genauer geht. Also nicht eine rechtliche Subsumtion, sondern können Sie uns berichten, wie die Auswahl geht, wer drüberguckt? Sind Ihnen Selektoren bekannt? Wenn uns ein Selektor eines Außenministers eines EU-Mitgliedstaates über den Weg laufen würde, wie kommt der da rein? Setzt das irgendein Client fest, sagt der: „Wir möchten mal eben hier als Unterabteilung CIA von der NSA den Außenminister des EU-Landes X als Selektor eingesteuert haben“, dann sagen die: „Super, für unseren Client tun wir alles“? Wie funktioniert das ganz konkret? Können Sie etwas dazu sagen? Also, keine abstrakte Subsumtion - da kämpfen wir auch schon mit deutschen Gesetzen, sie vernünftig zu subsumieren -, sondern ich würde gerne wissen: Wie läuft es ganz genau ab in der Praxis mit den Selektoren? - Das wäre eine Frage.

Und die zweite Frage dann wahrscheinlich stärker an Herrn Soghoian ausschließlich: Können Sie uns noch was von konkreten Operationen erzählen? Ich meine, das ist ja heute für uns eine große Chance, über die Vielzahl von Akten, Dokumenten, Einblicken, die wir bisher gewonnen haben, noch Neues zu erfahren. Wissen Sie über das hinaus, was Sie jetzt in diesem Untersuchungsausschuss hier verfolgen konnten - denn Sie haben ihn wahrscheinlich die letzten Monate auch immer mal wieder mit verfolgt -, über weitere Programme, Projekte der Kooperation,

Deutsche Übersetzung

Original

insbesondere mit Deutschland, etwas? Wissen Sie irgendetwas über Verfahren, die wir noch näher betrachten sollten in diesem Untersuchungsausschuss? Also sprich: Gucken Sie, was es bei uns Neues gibt, oder können Sie uns noch Neues sagen? Das würde mich natürlich interessieren. Ich möchte die Chance nicht ungenutzt lassen, dass wir von Ihnen noch Hinweise kriegen, wo wir genauer hingucken sollen. Schreiben an die amerikanische Regierung ist zwar immer hoffnungsvoll von uns - die amerikanische Regierung hilft uns auch das eine oder andere Mal -,

(Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Wo? Keine einzige Frage beantwortet!)

aber Sie können uns vielleicht noch weitere Türen öffnen. Und deswegen würde mich das interessieren.

Sachverständiger Timothy H. Edgar: Thank you. - I guess this is probably a good opportunity to say, since you warned me of the criminal penalties of lying to this committee, that I am under potential criminal penalties if I told you specific selectors that the NSA has under surveillance. And luckily I don't have that information anyway.

But in terms of how selectors might be acquired, it's really simply a matter of intelligence gathering; that is the craft of intelligence. And you gave an example that I think is a fairly realistic one, actually, of another agency saying, This is a person of intelligence interest to us. Can you please monitor them? We have a selector. Please run this through your systems. - Yeah, that's essentially how it would work.

Deutsche Übersetzung

Sachverständiger Timothy H. Edgar: *Vielen Dank. - Ich denke, dies ist wahrscheinlich eine gute Gelegenheit, Ihnen mitzuteilen - da Sie mich auf die strafrechtlichen Konsequenzen einer Falschaussage vor diesem Ausschuss hingewiesen haben -, dass mir strafrechtliche Konsequenzen drohen, wenn ich Ihnen spezifische Selektoren nenne, die die NSA überwacht. Zum Glück entzieht sich das ohnehin meiner Kenntnis.*

Was jedoch die Frage angeht, wie solche Selektoren ermittelt werden: Das ist ganz einfach eine Frage der Informationsgewinnung, das ist das Handwerk der Nachrichtendienste. Sie haben ein Beispiel genannt, das tatsächlich ziemlich realistisch ist, dass nämlich eine andere Behörde sagt: Diese Person ist für uns von nachrichtendienstlichem Interesse. Würden Sie sie bitte überwachen? Wir haben einen Selektor. Lassen Sie den doch bitte durch Ihre Systeme laufen. - Ja, im Wesentlichen funktioniert es genau so.

Nur zur dienstlichen Verwendung

Original

Now, it would be important for the analyst, when considering a selector, to consider a few different questions. One is: Is this selector likely to produce foreign intelligence that is responsive to a priority that the NSA has been given as part of the National Intelligence Priorities Framework, which is a yearly process that was described in one of the statements to just say, "These are the areas of intelligence that we care about"? And that's supposed to weed out certainly things like the abuses that Dr. Soghoian discussed. You would also look at what we call the "foreignness determination". So, is there information about where this person might be located? Either technical information the NSA may already have in its databases, information that is why we got this selector in the first place, things like that. And so you'd want to make sure that it was reasonably likely that that was a foreign selector.

Just to be clear about what would happen if there was a mistake on that question: yes, you could make a mistake, and it could be an American selector that you didn't realize was American. As you continue to collect intelligence, if you figure this out, you have to immediately detask the selector. So, sometimes people don't really get this. It's actually a very important point: you don't know necessarily where the person is right now when you begin surveillance, but as you continue surveillance, you will find out a lot of information about that person. And therefore, when you put in place a check that says that you must be reasonably sure that this person is overseas before you even begin collection, that's actually a fairly - - you know, that's not always an easy thing to do. But it becomes much easier afterwards. So there is a way to kind of mitigate the damage of mistakes that might happen.

Deutsche Übersetzung

Für den Analysten, der einen Selektor in Betracht zieht, ist es wichtig, mehrere Fragen zu berücksichtigen. Eine Frage lautet: Ist es wahrscheinlich, dass dieser Selektor Auslandsinformationen liefert, die für eine der Prioritäten im National Intelligence Priorities Framework der NSA genutzt werden können? Die Prioritäten sind Teil dieses Frameworks, das die NSA jährlich erstellt und dessen einzige Aussage in einer der Stellungnahmen folgendermaßen beschrieben wurde: Dies sind die Bereiche der Aufklärung, die uns interessieren. - Und damit sollen sicher Dinge wie die Missbrauchsfälle ausgemerzt werden, die Dr. Soghoian beschrieben hat. Außerdem würde man berücksichtigen, was wir die „foreignness determination", die „Feststellung des Ausländischen", nennen. Gibt es also Informationen darüber, wo sich diese Person aufhält? Das können entweder technische Informationen sein, die bereits in den Datenbanken der NSA vorliegen, [oder] Informationen, deretwegen wir den Selektor überhaupt erst haben, so etwas in der Art. Man wird also möglichst sicherstellen, dass Grund zu der Annahme besteht, dass es sich um einen ausländischen Selektor handelt.

Nur um klarzustellen, was geschehen würde, wenn in diesem Punkt ein Fehler gemacht wird: Ja, man kann sich täuschen, und es könnte sein, dass es sich um einen amerikanischen Selektor handelt, bei dem einem nicht klar war, dass er amerikanisch ist. Wenn man dies im Laufe der Informationserfassung feststellt, muss man den Überwachungsauftrag für diesen Selektor umgehend stoppen. Manche Leute verstehen das nicht ganz. Es ist aber ein sehr wichtiger Punkt. Man weiß vielleicht nicht genau, wo sich die Person zu dem Zeitpunkt aufhält, zu dem man mit der Überwachung beginnt; aber im Laufe der Überwachung erhält man sehr viele Informationen über die Person. Wenn man daher eine Bedingung setzt, wonach man vor Beginn der Überwachung Grund zur Annahme haben muss, dass sich die Person im Ausland aufhält, dann ist das eigentlich ziemlich - - das ist nicht immer einfach zu bewerkstelligen. Später wird es jedoch einfacher. Also gibt es einen Weg, den Schaden

Original

And other kinds of selectors are generated through the internal process within the agency from metadata, from analysis of chaining metadata records, so you know that these people are very important in a particular network, let's say a terrorist network or a weapons proliferation network, and they all seem to be talking to this one over here that you don't have under coverage. You would want to put that person under coverage; you'd want to put that selector into the list. And that's where a lot of the need for bulk collection comes from: it's to have that kind of database available to find those contacts.

So, again, as with my answer to Mr. von Notz, I'm not sure how much reassurance this is giving you about the process. You know, this is what makes intelligence gathering on a mass scale much different from targeted law enforcement operations or even targeted intelligence operations inside the country, where you have a lot more restrictions as to what you can do. And, you know, having laws and processes in place - - To me, I think, the greatest contribution that Snowden has given us and the opportunity that he has given us, is to have the conversation we're having right now about what kinds of protections, what kinds of oversight should apply to such massive programs that really don't operate in the way that we as lawyers expect surveillance to operate.

And we could do one of two things, it seems to me -or at least three things perhaps. We could say, We don't agree with this way of operating. We think this is mass surveillance and these programs should be shut down and that only targeted surveillance should take place. - You might say, We're totally comfortable with this, because we think we're doing the right thing to protect the country. - I think there is something

Deutsche Übersetzung

einigermaßen zu begrenzen, der sich hier aus möglichen Irrtümern ergibt.

Andere Arten von Selektoren werden durch den internen nachrichtendienstlichen Prozess generiert - aus Metadaten, aus Analysen aufgezeichneter Metadatenketten, denen man entnimmt, dass diese bestimmte Leute in einem bestimmten Netzwerk, beispielsweise einem Terroristennetzwerk oder einem Waffenhandelsnetzwerk, besonders bedeutend sind und alle mit dieser einen Person in Verbindung zu stehen scheinen, die man bisher nicht überwacht. Diese Person sollte man dann auch überwachen; also sollte man den Selektor auf die Liste setzen. Ein Großteil des Bedarfs an massenhaft erfassten Daten rührt daher, dass man eine Datenbasis zur Verfügung haben will, anhand derer sich solche Kontakte ausfindig machen lassen.

Ähnlich wie bei einer Antwort an Herrn von Notz bin ich nicht sicher, inwieweit das Ihre Bedenken hinsichtlich des Verfahrens ausräumt. Wissen Sie, darin unterscheidet sich die massenhafte Erfassung von Aufklärungsinformationen von gezielten Strafverfolgungsoperationen oder sogar gezielten nachrichtendienstlichen Operationen im Inland, wo man in seinem Handlungsspielraum viel eingeschränkter ist. Und wenn man Gesetze und Verfahren hat - - In meinen Augen besteht der größte Beitrag, den Snowden geleistet hat und besteht die große Chance, die er uns eröffnet hat, darin, dass wir genau die Gespräche führen, die wir gerade führen - darüber, welche Art von Schutz und welche Art von Kontrolle für solche massiven Programme gelten sollen, die nicht wirklich so funktionieren, wie wir als Anwälte es von Überwachung erwarten.

Und wir können zweierlei tun, scheint mir - oder vielleicht sogar dreierlei. Wir können sagen: Wir sind nicht einverstanden damit, wie sie funktionieren. Wir sind der Meinung, dass das Massenüberwachung ist und diese Programme eingestellt und nur noch gezielte Überwachungsmaßnahmen durchgeführt werden sollen. - Oder wir sagen: Wir finden das vollkommen in Ordnung, denn wir sind der Meinung, dass wir damit das

Original

in the middle that says, We think these programs have important capabilities that we don't want to give up, but we do want to have greater oversight of how they operate, because they are subject to more types of abuse than the targeted types of programs are.

Sachverständiger Dr. Christopher Soghoian: So I'll try to answer the second question. But on the issue of selectors, one pretty useful and interesting anecdote from one of the Snowden stories relates to an incident a few years ago when the NSA accidentally spied on telephone calls in Washington, D.C. An analyst was attempting to enter an Egyptian target into the system. Egypt's country code is 20. The analyst made a mistake. The Washington, D.C., area code is 20, too, and so NSA accidentally swept up Washington, D.C., based communications while attempting to spy in Egypt. I think it's just a useful data point that you can make a mistake and accidentally get the wrong person. This happens, of course, in the law enforcement context when the police search the wrong house. But it's a very different story when you're collecting vast quantities of communications.

With regard to your question about what should this committee do: you have the power to demand answers from domestic companies. If I were in your shoes, I would look to Germany's surveillance industry. So, there are a number of companies in your country - Gamma, Trovicor, which was spun out from Nokia Siemens - who export surveillance technology to some of the most authoritarian countries in the world. When it comes to surveillance, Germany is not innocent; you have a lot of blood on your hands. You are enabling surveillance by some of the worst regimes in the world, and I think it would be pretty useful to go and request the customer lists

Deutsche Übersetzung

Richtige tun, um unser Land zu schützen. - Ich denke, es gibt noch etwas dazwischen, nämlich zu sagen: Wir sind der Meinung, dass diese Programme wichtige Möglichkeiten bieten, auf die wir nicht verzichten möchten, aber wir wollen bessere Kontrolle darüber haben, wie sie ablaufen, denn sie werden auf vielfältigere Weise missbraucht als die gezielten Überwachungsprogramme.

Sachverständiger Dr. Christopher Soghoian: *Ich werde versuchen, die zweite Frage zu beantworten. Was jedoch die Frage der Selektoren betrifft, so gibt es eine ziemlich erhellende und interessante Anekdote in einer der Snowden-Geschichten, in der es um einen Vorfall vor einigen Jahren geht, als die NSA versehentlich Telefonate in Washington, D. C. überwachte. Ein Analyst wollte eine ägyptische Zielperson ins System eingeben, und die Landesvorwahl von Ägypten ist 20. Der Analyst machte einen Fehler. Die Ortsvorwahl von Washington, D. C. ist ebenfalls 20, und so fischte die NSA versehentlich Kommunikationsdaten aus Washington, D. C. ab, während sie eigentlich versuchte, in Ägypten zu spionieren. Ich denke, es ist einfach wichtig, zu wissen, dass man einen Fehler machen und versehentlich die falsche Person erwischen kann. Dasselbe geschieht natürlich auch im Rahmen der Strafverfolgung, wenn die Polizei die falsche Wohnung durchsucht. Aber wenn man Riesenmengen an Kommunikationsdaten erfasst, ist das eine ganz andere Geschichte.*

Bezüglich Ihrer Frage, was dieser Ausschuss tun sollte: Sie haben die Macht, Antworten von inländischen Unternehmen einzufordern. An Ihrer Stelle würde ich mir die deutsche Überwachungsbranche vornehmen. Es gibt in diesem Land eine Reihe von Unternehmen, darunter Gamma und trovicor - ein Ableger von Nokia Siemens -, die Überwachungstechnologie an einige der autoritärsten Staatssysteme der Welt liefern. Deutschland ist kein Unschuldslamm, was die Überwachung angeht. Sie haben sehr viel Blut an den Händen. Sie ermöglichen die Überwachung durch einige der weltweit schlimmsten Regime, und ich denke, es wäre

Original

and the contracts from these companies and figure out who has purchased equipment and which particular surveillance capabilities you have allowed to be exported around the world.

Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank für diesen Hinweis. - Frau Kollegin Renner hatte sich noch gemeldet.

Martina Renner (DIE LINKE): Ich habe noch zwei kurze Fragen. Die erste geht vielleicht an Herrn Halperin, weil er sich ja intensiv auch mit der Frage Presse und Geheimdienste befasst hat, knüpft aber an die ganze Selektorenproblematik an, die meine Vorfragenden schon aufgeworfen haben. Gibt es Schutzmechanismen, die ausschließen, dass Selektoren gegen Berufsgeheimnisträger gerichtet werden, also gegen Rechtsanwälte, Rechtsanwältinnen, gegen Pressevertreter, Geistliche, Ärzte? Das ist auch eine Frage. Wenn uns sozusagen jetzt hier aufgegeben ist, wir müssen ja die NSA-Selektoren und die BND-Selektoren anschauen hinsichtlich der Fragestellung „Was liegt außerhalb des Auftragsprofils des Bundesnachrichtendienstes? War es ungesetzlich?“, spielt möglicherweise ja auch die Frage eine Rolle, wo es gegebenenfalls solche Schutzmechanismen geben könnte. Gibt es die bei der NSA? Gibt es Berufsgruppen, die ausgenommen sind bei der Überwachung? - Das wäre meine erste Frage.

Und die zweite an Amie Stepanovich: Sie haben ja in Ihrer schriftlichen Ausarbeitung auf so einige Probleme in der US-Gesetzgebung hingewiesen. Da geht es um die Definition von „bulk surveillance“. Was mich aber mehr interessiert, ist die Problematik, die Sie aufwerfen bei dem Begriff der „collection“, weil dort ja die Daten nicht geschützt sind, solange sie durchs Computersystem laufen und erst mal nur zum Beispiel durchsucht werden, also zum Beispiel mit Selektoren, und danach dann gelöscht werden oder entschieden wird, ob man sie weiter verarbeitet. So eine Auseinandersetzung kennen wir hier zum Teil auch. Es haben auch Zeugen

Deutsche Übersetzung

ziemlich hilfreich, wenn Sie die Kundenkarteien und Verträge dieser Unternehmen einforderten und herausfänden, wer Technologie eingekauft hat und für welche technischen Möglichkeiten Sie den weltweiten Export gestattet haben.

Original

aus dem BND vorgetragen, dass sie die Rechtsauffassung haben, solange die Daten wie in einem Strom nur mit einem Netz durchsucht werden, würde zum Beispiel bei uns das Bundesdatenschutzgesetz noch nicht greifen. Gibt es da Diskussionen, so was zu verändern, oder ist das also gesetzt, statisch, und wird es auch in Zukunft dabei bleiben, dass man diese Rechtsauffassung in den USA hat? - Danke.

Sachverständiger Dr. Morton H. Halperin: The first point is: nobody is exempt from surveillance or being put on a whitelist because you're a minister or a doctor or a lawyer. Certain conversations would be subject to minimization procedures; I think for the moment only if they're U.S. persons. I don't think the President's Directive extends that protection, but I'm not certain of that. But then the third point is: there are always exceptions to the exception. To say, if there's evidence of a crime, if there's a direct threat to life or property, you can use the information to a limited degree. So there's some protection, but not a great deal.

Sachverständige Amie Stepanovich: In regard to the definition of collection: the U.S. government actually just reissued the document that contains that definition, and they changed it to reflect the definition that I included in my testimony. That had been the policy for a very long time; it is now specifically written in the definition of that document in order to preserve, we believe, the Section 702 program and their claim under it. Notably, that definition - - Something that I find quite interesting is that they key it to the amount of time that they hold on to the information and scan it. So they talk about how it's momentarily held in order to conduct the scanning. With the current technology - not to mention technology available in the future - the time held is actually not necessarily representative of the amount of information that they can get out of that data. We have computing power to do a tremendous amount of scanning with

Deutsche Übersetzung

Sachverständiger Dr. Morton H. Halperin: *Zur ersten Frage: Niemand wird von der Überwachung ausgenommen oder auf eine weiße Liste gesetzt, weil er Geistlicher oder Arzt oder Anwalt ist. Bestimmte Gespräche wären Gegenstand von Minimierungsverfahren. Ich glaube, bisher gilt das nur, wenn es sich um US-Personen handelt. Ich glaube nicht, dass die Direktive des Präsidenten diesen Schutz bietet, aber da bin ich nicht sicher. Der dritte Punkt ist jedoch, dass es immer Ausnahmen von der Ausnahme gibt. Das heißt, wenn Hinweise auf eine Straftat vorliegen und eine direkte Bedrohung für das menschliche Leben oder Sachwerte besteht, dann kann man diese Informationen bis zu einem bestimmten Grad nutzen. Es gibt also einen gewissen Schutz, aber keinen sehr großen.*

Sachverständige Amie Stepanovich: *Was die Definition von Datenerfassung betrifft: Die US-Regierung hat erst vor kurzem das Dokument, in dem diese Definition enthalten ist, neu aufgelegt. Sie wurde so verändert, dass sie nun der Definition entspricht, die ich in meiner Stellungnahme genannt habe. Dies entspricht schon lange der Vorgehensweise und wurde nun gezielt in die Definition dieses Dokuments aufgenommen, um, so glauben wir, das §-702-Programm und ihre Ansprüche im Rahmen dieses Programms zu erhalten. Bemerkenswert an dieser Definition - - Was ich sehr interessant finde, ist, dass sie es an der Zeitdauer festmachen, für die sie die Informationen speichern und scannen. Sie geben also an, wie lange sie die Daten aktuell aufbewahren, um sie scannen zu können. Mit der heute verfügbaren Technologie - ganz zu schweigen von zukünftigen technologischen*

Original

only moments to scan. And so they are able to look at entire communications. They potentially may be able to analyze those communications and conduct other forms of analysis that are more invasive in order to determine not only exactly what words are in it, but what it's talking about in general, kind of non-specific details of the communication.

And so, if we continue to key how long communications can be held as to whether or not they are collected, what we are going to find out in the future is that more and more data can be gleaned from those communications through this type of analysis really with only holding the information momentarily and then immediately discarding it. This allows for what we would absolutely call "mass surveillance" - absolutely -, but we think that the U.S. should term it "bulk surveillance", because the actual scanning of the communications is happening without discrimination. The discrimination - the piece that makes it targeted and not bulk - is what happens during the scan. And we think that is very disingenuous. It definitely has come up several times while I was talking to EU lawmakers about the Privacy Shield negotiations, where they were told on several occasions that Section 702 surveillance was targeted, and we had to explain what that meant, because "targeted" means something very different under EU law and under U.S. law.

Vorsitzender Dr. Patrick Sensburg: Okay. - Ich schau mal. Ich habe nur noch mal eine kleine Nachfrage an Herr Soghoian. Eine Firma habe ich mir merken können. Können Sie noch ein bisschen mehr zu den deutschen Unternehmen im Bereich der - -

Deutsche Übersetzung

Möglichkeiten - sagt die Dauer der Datenaufbewahrung nicht zwangsläufig etwas darüber aus, wie viele Informationen sie aus diesen Daten gewinnen können. Mit leistungsstarken Rechnern lässt sich in kürzester Zeit enorm viel scannen. Also können sie sich gesamte Kommunikationen ansehen. Sie können diese Kommunikationen möglicherweise analysieren und auch weitere Arten von Analysen durchführen, die noch tiefer eindringen, um nicht nur den Wortlaut zu ermitteln, sondern auch das allgemeine Thema, also eher nichtspezifische Einzelheiten der Kommunikation.

Wenn wir die Definition, ob Kommunikationsdaten erfasst werden oder nicht, daran festmachen, wie lange sie aufbewahrt wurden, dann werden wir zukünftig feststellen, dass sich mit dieser Art von Analyse mehr und mehr Informationen aus diesen Daten gewinnen lassen, obwohl sie nur sehr kurz aufbewahrt und anschließend sofort gelöscht wurden. Das ermöglicht das, was wir unbedingt als Massenüberwachung bezeichnen würden, unbedingt. Wie sind jedoch der Ansicht, dass die USA es „Bulk Surveillance" nennen sollten, weil das Scannen der Kommunikation selbst ohne jede Unterscheidung geschieht. Die Unterscheidung - also der Teil, der aus Massenüberwachung gezielte Überwachung macht - erfolgt erst beim Scannen. Und das halten wir für sehr unaufrichtig. Als ich mit EU-Gesetzgebern über die Verhandlungen zum EU-US Privacy Shield sprach, kam dieses Thema mehrfach auf. In den Verhandlungen wurde den EU-Gesetzgebern verschiedentlich gesagt, dass die Überwachung nach § 702 gezielt sei, und wir mussten erklären, was das bedeutet, denn EU-Recht definiert „gezielt" ganz anders als US-Recht.

Original

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Wir haben einen Gesetzesentwurf dazu geschrieben! Den könnte ich dir zukommen lassen!)

- Ja, das wissen wir ja im Zweifel schon. Aber was der Herr Soghoian noch zusätzlich weiß. Vielleicht ist da ja noch mehr drin als bei euch. - Mich würde natürlich interessieren: Welche Firmen haben Sie da noch in petto? Also, was Sie uns jetzt berichten könnten - ich schreibe das mit -, das wäre interessant für uns.

Sachverständiger Dr. Christopher Soghoian: That would be great; it would be great for you to take notes and to launch an investigation. So, the two companies I recommend that you look at: one is called Gamma, G - A - M - M - A. They make a famous spyware product called FinFisher or FinSpy. And then the other company is called Trovicor, T - R - O - V - I - C - O - R. They were spun out of Nokia Siemens. They also make bulk surveillance technology. These are just two of the companies that manufacture this technology, but you could, of course, also talk to the respective agency within your government that grants export licenses for surveillance technology to find out which other domestic German companies are exporting surveillance technologies to authoritarian regimes around the world.

Vorsitzender Dr. Patrick Sensburg: Okay, gut. - Ich schaue mal, ob es weitere Fragen gibt. - Ich sehe, momentan haben wir keine weiteren Wortmeldungen. Vielleicht komme ich noch mal bilateral auf Sie zu. Aber gut.

Wenn es keine weiteren Fragen mehr gibt, die jetzt in öffentlicher Sitzung gestellt werden können, dann sind wir am Ende der Anhörung mit Ihnen, meine Damen und Herren. Eine Information: Nach seiner Fertigstellung wird Ihnen vom Sekretariat das Stenografische Protokoll übersandt, das wir ja von dieser Sitzung anfertigen. Sie haben dann, wie ich es zu Anfang gesagt

Deutsche Übersetzung

Sachverständiger Dr. Christopher Soghoian: *Das wäre großartig, wenn Sie das mitschreiben und eine Untersuchung einleiten würden. Also, die beiden Unternehmen, die Sie sich ansehen sollten: Das eine heißt Gamma: G - A - M - M - A. Sie stellen ein sehr bekanntes Spyware-Produkt her, FinFisher bzw. FinSpy. Das andere Unternehmen heißt trovicor: T - R - O - V - IC - O -R. Das ist ein Ableger von Nokia Siemens. Sie stellen ebenfalls Technologie zur massenhaften Überwachung her. Dies sind nur zwei Unternehmen, die solche Technologie herstellen; aber Sie können natürlich auch die zuständige staatliche Behörde ansprechen, die Exportlizenzen für Überwachungstechnologie ausstellt, um herauszufinden, welche anderen deutschen Inlandsunternehmen Überwachungstechnologien an autoritäre Regime weltweit liefern.*

Original

habe, zwei Wochen Zeit, etwaige Korrekturen an der Übertragung vorzunehmen oder Richtigstellungen oder Ergänzung Ihrer Aussage, wenn irgendetwas im Protokoll nicht so sein sollte, wie Sie es gesagt haben.

Ich darf mich am Ende ganz herzlich bei Ihnen bedanken, dass Sie den weiten Weg auf sich genommen haben, uns Rede und Antwort gestanden haben für viele Fragen, die uns, glaube ich, in der Gesamtschau und Bewertung dieses gesamten Themenkomplexes wichtige Hilfen sind. Ich bedanke mich für Engagement, dass Sie im Rahmen dieser ganzen Thematik immer wieder für uns Ansprechpartner sind - in Washington waren es ja schon einige von Ihnen -, und darf mich insgesamt bedanken, dass Sie so lange mit uns ausgeharrt haben. Die Sitzungen hier sind immer lang. Ganz herzlichen Dank für das alles. Danke schön.

Die Sitzung ist damit geschlossen. Die nächste Ausschusssitzung findet voraussichtlich am 22. September 2016 statt. Der Öffentlichkeit, den Vertretern der Medien darf ich heute auch wieder danken für die intensive Teilnahme und die Berichterstattung von diesem Ausschuss. Damit ist diese Sitzung geschlossen. Für uns findet jetzt noch eine kurze Beratungssitzung statt. Die ist aber natürlich wie immer nicht mit der Öffentlichkeit, sondern unter uns, unter Ausschluss der Öffentlichkeit. Allen einen schönen Abend noch. Und die Ausschussmitglieder, die Bundesregierung und alle, die an der Beratungssitzung teilnehmen, die bitte ich jetzt, hier zu warten, bis der Saal dementsprechend wieder frei ist. Danke schön. Schönen Abend.

(Schluss: 17.06 Uhr)

Deutsche Übersetzung

ANLAGE 1

Notably, the Foreign Intelligence Surveillance Act Amendments Act, or FAA, which includes Section 702, which, as my colleague Ashley Gorski has explained, contains both authority for Prism and Upstream, will sunset late next year. Which means we're in the same situation we were with Section 215, ~~where it~~part of the USA PATRIOT Act that ~~sunsetted~~ had a sunset date last year. Because of the sunset ~~and where~~ we were able to get the political will to pass the USA Freedom Act to ~~limit~~ reform that authority. However, Congress has not even begun really to discuss what the reform of Section 702 and the other FAA provisions will look like. And what it seems that we are most likely to get out of that sunset is a limitation on the search of 702 databases for U.S. person information without a warrant, and not necessarily to the limits of data collected of non-U.S. persons.

And then, in the law enforcement context, surveillance authorities are potentially increasing.

I'd like to draw your attention to a draft law that was recently published to amend the Electronic Communications Privacy Act in order to allow bilateral agreements between countries with the goal of providing direct, reciprocal access for other governments to order the production of user information from companies located in ~~other jurisdictions~~the United States. The draft law would be precedent-setting in the United States, in that it will actually write human rights into U.S. statute, but the standard for the human rights is too weak. So, to understand why, I want to indicate that the first country that the U.S. is likely to enter into an agreement with under this draft law is the United Kingdom, the home to GCHQ. The UK already has arguably much broader surveillance authorities with much less oversight than the ~~U.S. National Security Agency.~~United States. And once passed - and it's being taken back up again tomorrow in the UK House of Lords - the Investigatory Powers Bill will give even broader authority with only the illusion of oversight. Whilst the agreement between the U.S. and the UK would ensure some protections for their own citizenry, they would not include any protections for citizens located elsewhere in the world, including Germany. This will not change the substance of surveillance authority, but it will give current and future authorities a much broader application, ~~to undermine~~undermining the privacy of users around the world by allowing the UK to get direct access to information of Germans held by U.S. companies without going through mutual legal assistance treaties, as is now the case.

Several of my colleagues have also brought up the Schrems case. ~~And one important limitation —~~My colleague Mr. Edgar talked about how the Schrems case will allow another opportunity for Europeans to press for reform. But I actually think that that opportunity has been severely limited by the U.S. Congress. This is because of a last minute change made in the passage of the Judicial Redress Act or JRA ~~they actually took a very last-minute step in the passage of the Judicial Redress Act, or the JRA~~. Many of you might be familiar with the JRA. It was a necessary precondition to the adoption of the U~~u~~mbrella A~~a~~greement between the EU and the United States. And it was supposed to extend certain U.S. Privacy Act protections to EU citizens, so that they could have some guarantee of protection and redress against U.S. government

collection of their data. We at, Access Now, had indicated that the JRA was going to be a small step forward for the rights of Europeans within the Unites States. However, at the very last minute, the U.S. Senate actually gutted that protection, and what would have been half a step forward became a huge step back. What happened was that theSpecifically, Senator Cornyn attached an amendment that was adopted statinge included a provision that said that no country could qualify for the Privacy Act protections which if it had impeded the national security interests of the United States. This means thatConsequently, if the EU starts to place pressure on the United States to limit its surveillance of EU citizens, EU countries could find themselves stripped of their ability to get JRA status, which means thatand even the limited redress that has been provided could be taken away. This not only means that in the Privacy Shield negotiations EU interests were severely hampered, but in the future they will continue to be hampered and they will continue to be limited in how much they can exert pressure on U.S. surveillance.

In the U.S., Senators Burr and Feinstein have recently drafted the Compliance with Court Orders Act of 2016, which could be introduced at any time - to disastrous consequences. It will likely lead to greater crime, more compromised information, and both more prosecutionpersecution,s and possibly deaths, of journalists and activists in repressive countries. What this and other mandates sought and will not do, however, is limit the use of encryption by terrorists and criminals. These actors - to whom that we most want to limit the use of tools that law enforcement cannot gain access to - will still have available to them open source tools, tools that they developed themselves as well as tools developed in other countries to which jurisdiction does not reach. It will only have a primary impact of limiting the amount of security available to everyday citizenry, including the most at-risk users.

And finally, a word on government hacking, because both the FBI and the NSA have entire units devoted to government hacking. And the FBI is now seeking a procedural rule change, in fact, a rule change that will go into effect at the beginning of December of this year, unless Congress acts. So, they have switched the presumption: Congress does not have to act to change the rule; they simply have to do nothing, and the change goes into effect. Senator Wyden is on the floor of the U.S. Congress, I believe, today in order to try to pass legislation that would stop this change, with the Stopping Mass Hacking Act. But the ability for Congress to act this year, because of the U.S. elections, is going to be limited. And the rule change will ostensibly give the FBI authority the means to hack into computers around the world, so long as they don't know where the computer is located. Right now, the FBI has no substantive authority under U.S. law to hack; in fact, Congress has never spoken to this issue in U.S. law.

Sachverständige ~~Amie Stepanovich~~Ashley Gorski: Excuse me, Dr. Sensburg. Could we actually get a break now before the questions begin?

Sachverständige Amie Stepanovich: Thank you very much. - I think the primary expectation that we have for all governments, including that in Germany, is to effectively implement what we call the "International Principles on the Application of Human Rights to Communications Surveillance". This is a set of 13 principles that ha~~ve~~s been agreed to by organizations and some governments around the world, available at necessaryandproportionate.org, ~~that~~ which we believe represent what is currently written already into human rights law and policy - both through court findings, policy documents, and generally understood interpretations of law.

Access Now has published an implementation guide on what we think laws that adequately protect human rights would look like under those principles ~~--~~ ~~so trying to engage in~~ with the goal of kick-starting a realistic conversation about to what extent and how laws can be passed that protect human rights, that provide for adequate notice to users about when they can be subject to surveillance, both users within Germany and users around the world, and then to provide a common standard for both to make sure that extraterritorial surveillance does not happen in a way that violates other users' rights or that undermines Internet security globally.

Sachverständige Amie Stepanovich: In regard to the definition of collection: the U.S. government actually just reissued the document that contains that definition, and they changed it to reflect the definition that I included in my testimony. That had been the policy for a very long time; it is now specifically written in the definition of that document in order to preserve, we believe, the Section 702 upstream program ~~and their claim under it~~. Notably, ~~that~~ the new official definition ~~- - Something that I find quite interesting is that they key~~is keyed ~~it~~ to the amount of time that they hold on to the information ~~and scan it~~. So they talk about how it's momentarily held in order to conduct the scanning. With the current technology - not to mention technology available in the future - the time held is actually not necessarily representative of the amount of ~~information~~ analysis that they can ~~get out of that~~perform on the data. We have computing power to do a tremendous amount of ~~scanning~~ analysis and derive a lot of information with only moments to scan. And so they are able to look at ~~entire communications~~all internet traffic. They potentially may be able to analyze ~~those~~ all communications and conduct other forms of analysis that are more invasive in order to determine not only exactly what words

are in it, but what it's talking about in general, kind of non-specific details of the communication.

And so, if we continue to key how long communications can be held as to whether or not they are collected, what we are going to find out in the future is that more and more data can be gleaned from those communications through this type of scanning and analysis really with only holding the information momentarily and then immediately discarding it. This will ~~allows~~facilitate ~~for~~ what we would absolutely call "mass surveillance" ~~-~~– absolutely. It also should constitute what the U.S. government refers to as "bulk surveillance," meaning indiscriminate surveillance, since ~~-, but we think that the U.S. should term it "bulk surveillance", because~~ the actual scanning of the communications is happening without discrimination. The discrimination - the piece that makes it targeted and not bulk - is what happens during the scan. And we think pretending otherwise ~~that~~ is very disingenuous. It definitely has come up several times while I was talking to EU lawmakers about the Privacy Shield negotiations, where they were told on several occasions that Section 702 surveillance was targeted, and we had to explain what that meant, because "targeted" means something very different under EU law and under U.S. law.