Humanistische Union

Internationale Grundsätze für die Anwendung der Menschenrechte in der Kommunikationsüberwachung

Dank Edward Snowden und weiterer Whistleblower wissen wir inzwischen, dass die geheimdienstliche Überwachung der elektronischen Kommunikation in viel größerem Umfang stattfindet als bisher gedacht, und mit der Überwachungstechnik und den Ergebnissen der Überwachung reger Handel betrieben wird. Wir wissen seitdem aber auch, dass für eine effektive internationale Regulierung der Kommunikationsüberwachung noch die geeigneten rechtlichen Maßstäbe fehlen. Dieser Aufgabe stellt sich eine Erklärung zahlreicher NGOs und zivilgesellschaftlicher Initiativen. Sie formuliert einen Katalog einfacher menschenrechtlicher Mindestanforderungen an die internationale Kommunikationsüberwachung.

Während die Technologien, welche die staatliche Kommunikationsüberwachung unterstützen, verbessert werden, vernachlässigen die Staaten sicherzustellen, dass Gesetze und Verordnungen in Bezug auf Kommunikationsüberwachung in Einklang mit internationalen Menschenrechten stehen und die Rechte auf Privatsphäre und Meinungsfreiheit beachtet werden. Dieses Dokument versucht zu erklären, wie internationale Menschenrechte in der aktuellen digitalen Umgebung anwendbar sind, besonders vor dem Hintergrund des Wachstums und des Wandels der Technologien und Methoden der Kommunikationsüberwachung. Diese Grundsätze können zivilgesellschaftlichen Gruppen, der Wirtschaft, Staaten und anderen einen Rahmen liefern, mit dem sie bewerten können, ob aktuelle oder geplante Überwachungsgesetze oder -praktiken im Einklang mit den Menschenrechten stehen.

Diese Grundsätze sind das Ergebnis einer globalen Beratung mit Gruppen der Zivilgesellschaft, der Wirtschaft und internationalen Experten für Recht, Politik und Technologien in der Kommunikationsüberwachung.

Einleitung

Privatsphäre ist ein Grundrecht, das wesentlich ist für den Erhalt von demokratischen Gesellschaften. Es ist grundlegend für die menschliche Würde und verstärkt andere Rechte, wie Meinungs-, Informations- und Versammlungsfreiheit, und es ist nach internationalen Menschenrechtsgesetzen anerkannt.(1) Aktivitäten, die das Recht auf Privatsphäre begrenzen, einschließlich Kommunikationsüberwachung, können nur dann als gerechtfertigt gelten, wenn sie gesetzlich vorgeschrieben sind, sie notwendig sind, um ein legitimes Ziel zu erreichen, und sie dem Ziel, welches sie verfolgen, angemessen sind.(2)

Vor der öffentlichen Einführung des Internets schufen fest etablierte legale Grundsätze und der Kommunikationsüberwachung innewohnende logistische Hürden Grenzen für die staatliche Kommunikationsüberwachung. In gegenwärtigen Dekaden haben die logistischen Barrieren der Überwachung abgenommen und die Anwendung der gesetzlichen Grundsätze in neuen technologischen Kontexten sind unklarer geworden. Die Explosion der Inhalte digitaler Kommunikation und Information über Kommunikation, sogenannte „Verbindungsdaten“ - Informationen über die Kommunikation eines Individuums oder Nutzung elektronischer Geräte - die sinkenden Kosten der Speicherung und des Dataminings und die Bereitstellung von persönlichen Inhalten durch Drittanbieter machen staatliche

Überwachung in einem beispiellosen Ausmaß möglich.(3) Dabei haben Konzeptualisierungen der bestehenden Menschenrechtsgesetze nicht Schritt gehalten mit den modernen und sich verändernden Möglichkeiten der Kommunikationsüberwachung des Staates, der Fähigkeit des Staates, aus verschiedenen Überwachungstechniken gewonnene Informationen zu kombinieren und zu organisieren, oder der erhöhten Sensibilität der Informationen, die zugänglich werden.

Die Häufigkeit, mit der Staaten Zugang zu Kommunikationsinhalten und -metadaten suchen, steigt dramatisch – ohne angemessene Kontrolle.(4) Wenn Kommunikationsmetadaten aufgerufen und analysiert werden, kann damit ein Profil einer Person, einschließlich des Gesundheitszustandes, politischer und religiöser Ansichten, Verbindungen, Interaktionen und Interessen, erstellt werden. So werden genauso viele oder sogar noch mehr Details offengelegt, als aus dem Inhalt der Kommunikation erkennbar wäre.(5) Trotz des riesigen Potenzials für das Eindringen in das Leben eines Menschen und der abschreckenden Wirkung auf politische und andere Vereinigungen, weisen rechtliche und politische Instrumente oft ein niedrigeres Schutzniveau für Kommunikationsmetadaten auf und führen keine ausreichenden Beschränkungen dafür ein, wie sie später von Behörden verwendet werden, einschließlich wie sie gewonnen, geteilt und gespeichert werden.

Damit Staaten tatsächlich ihren internationalen menschenrechtlichen Verpflichtungen in Bezug auf Kommunikationsüberwachung nachkommen, müssen sie den im Folgenden genannten Grundsätzen entsprechen. Diese Grundsätze gelten für die Überwachung der eigenen Bürger eines Staates, die in seinem eigenen Hoheitsgebiet ausgeführt wird, sowie der Überwachung anderer in anderen Gebieten. Die Grundsätze gelten außerdem unabhängig vom Zweck der Überwachung - Strafverfolgung, nationale Sicherheit oder sonstige behördliche Ziele. Zudem gelten sie sowohl für die Aufgabe des Staates, die Rechte des Einzelnen zu respektieren und zu erfüllen, als auch für die Verpflichtung, die Rechte des Einzelnen vor Missbrauch durch nicht-staatliche Akteure, einschließlich der Wirtschaft, zu schützen.(6) Der private Sektor trägt die gleiche Verantwortung für die Wahrung der Menschenrechte, insbesondere in Anbetracht der Schlüsselrolle, die sie bei der Konzeption, Entwicklung und Verbreitung von Technologien spielt, und damit Kommunikation ermöglicht und bereitstellt und - wo erforderlich - mit staatlichen Überwachungsmaßnahmen zusammenarbeitet. Dennoch ist der Umfang der vorliegenden Grundsätze auf die Pflichten des Staates beschränkt.

Veränderte Technologie und Definitionen

„Kommunikationsüberwachung“ umfasst heutzutage die Überwachung, das Abhören, die Sammlung, Analyse, Nutzung, Konservierung und Aufbewahrung von, den Eingriff in oder Zugang zu Informationen, welche die Kommunikation einer Person in der Vergangenheit, Gegenwart oder Zukunft beinhaltet, reflektiert oder sich daraus ergibt. „Kommunikation“ beinhaltet Aktivitäten, Interaktionen und Transaktionen, die über elektronische Medien übertragen werden, wie z.B. Inhalte der Kommunikation, die Identität der an der Kommunikation Beteiligten, das Standort-Tracking, einschließlich IP-Adressen, die Uhrzeit und die Dauer der Kommunikation und Kennungen von Kommunikationsgeräten, die während der Kommunikation verwendet werden.

Traditionell wurde die Invasivität der Kommunikationsüberwachung auf Basis von künstlichen und formalen Kategorien bewertet. Bestehende rechtliche Rahmenbedingungen unterscheiden zwischen „Inhalt“ oder „Nicht-Inhalt“, „Teilnehmerinformation“ oder „Metadaten“, gespeicherten Daten oder Übertragungsdaten, Daten, die zuhause gespeichert werden oder die im Besitz eines dritten Diensteanbieters sind.(7) Allerdings sind diese Unterscheidungen nicht mehr geeignet, den Grad des Eindringens der Kommunikationsüberwachung in das Privatleben von Einzelpersonen und Verbänden zu messen. Während seit Langem Einigkeit darin besteht, dass Kommunikationsinhalte per Gesetz signifikanten Schutz verdienen wegen ihrer Fähigkeit, sensible Informationen zu offenbaren, ist es nun klar, dass andere Informationen aus

der Kommunikation - Metadaten und andere Formen der nicht-inhaltlichen Daten - vielleicht sogar mehr über eine Einzelperson enthüllen können, als der Inhalt selbst und verdienen daher einen gleichwertigen Schutz. Heute könnte jede dieser Informationsarten, für sich allein oder gemeinsam analysiert die Identität einer Person, deren Verhalten, Verbindungen, physischen oder gesundheitlichen Zustand, Rasse, Hautfarbe, sexuelle Orientierung, nationale Herkunft oder Meinungen enthüllen, oder die Abbildung einer Person mithilfe der Standortbestimmung, ihrer Bewegungen oder Interaktionen über einen Zeitraum,(8) ermöglichen oder auch von allen Menschen an einem bestimmten Ort, zum Beispiel bei einer öffentlichen Demonstration oder anderen politischen Veranstaltungen. Als Ergebnis sollten alle Informationen, welche sich aus der Kommunikation einer Person ergeben, diese beinhalten, reflektieren, oder über diese Person stattfinden, und welche nicht öffentlich verfügbar und leicht zugänglich für die allgemeine Öffentlichkeit sind, als „geschützte Informationen“ angesehen werden. Ihnen sollte dementsprechend der höchste gesetzliche Schutz gewährt werden.

Bei der Beurteilung der Invasivität der staatlichen Kommunikationsüberwachung ist es notwendig, dass beides betrachtet wird: sowohl das Potenzial der Überwachung, geschützte Informationen offenzulegen, sowie der Zweck, zu der der Staat die Information sammelt. Kommunikationsüberwachung, die voraussichtlich zur Offenlegung von geschützten Informationen führt, die eine Person dem Risiko der Ermittlung, Diskriminierung oder Verletzung der Menschenrechte aussetzen kann, wird eine ernsthafte Verletzung des Rechts des Einzelnen auf Privatsphäre darstellen und außerdem die Nutzung anderer Grundrechte untergraben, unter anderem das Recht auf freie Meinungsäußerung, Versammlungsfreiheit und politische Partizipation. Dies liegt darin begründet, dass diese Rechte erfordern, dass Menschen in der Lage sind, frei von der abschreckenden Wirkung der staatlichen Überwachung zu kommunizieren. Eine Festlegung sowohl des Charakters als auch der Einsatzmöglichkeiten der gesuchten Informationen wird somit in jedem Einzelfall notwendig.

Bei der Annahme einer neuen Technik der Kommunikationsüberwachung oder der Ausweitung des Anwendungsbereichs einer bestehenden Technik sollte der Staat sicherstellen, ob die Informationen, die wahrscheinlich beschafft werden, in den Bereich der „geschützten Informationen“ fällt, bevor er sie einholt, und sie zur Kontrolle der Justiz oder anderen demokratischen Kontrollorganen vorlegen. Wenn man bedenkt, ob eine Information, die man mithilfe von Kommunikationsüberwachung erhalten hat, auf die Ebene der „geschützten Informationen“ aufsteigt, sind sowohl die Form als auch der Umfang und die Dauer der Überwachung relevante Faktoren. Weil tiefgreifende oder systematische Überwachung die Fähigkeit hat, private Informationen weit über seine einzelnen Teile hinaus zu offenbaren, kann auch die Überwachung der nicht geschützten Informationen auf ein Niveau der Invasivität gelangen, das starken Schutz verlangt.(9)

Die Festlegung, ob ein Staat die Überwachung geschützter Kommunikation durchführen darf, muss im Einklang mit den folgenden Grundsätzen stehen.

Die Grundsätze

Gesetzmäßigkeit: Jede Beschränkung des Rechtes auf Privatsphäre muss gesetzlich vorgeschrieben sein. Der Staat darf in Abwesenheit eines bestehenden öffentlich verfügbaren Rechtsaktes, welcher den Standard der Klarheit und Genauigkeit erfüllt, und der ausreicht, um sicherzustellen, dass Einzelne eine Benachrichtigung erhalten und seine Anwendung vorhersehen können, keine Maßnahmen einführen oder durchsetzen, die das Recht auf Privatsphäre beeinträchtigen. Angesichts der Geschwindigkeit des technologischen Wandels sollten Gesetze, die das Recht auf Privatsphäre beschränken, regelmäßig durch Instrumente eines partizipativen, legislativen und behördlichen Prozesses überprüft werden.

Rechtmäßiges Ziel: Gesetze sollten nur Kommunikationsüberwachung durch spezifizierte Behörden erlauben, um ein legitimes Ziel zu erreichen, welches einem überragend wichtigen Rechtsgut, das in einer

demokratischen Gesellschaft notwendig ist, entspricht. Es darf keine Maßnahme angewendet werden, die auf der Grundlage von Rasse, Hautfarbe, Geschlecht, Sprache, Religion, politischer oder sonstiger Überzeugung, nationaler oder sozialer Herkunft, Vermögen, Geburt oder des sonstigen Status diskriminiert.

Notwendigkeit: Gesetze, die Kommunikationsüberwachung durch den Staat erlauben, müssen die Überwachung darauf begrenzen, was zweifellos und nachweislich notwendig ist, um das legitime Ziel zu erreichen. Kommunikationsüberwachung darf nur durchgeführt werden, wenn es das einzige Mittel zur Erreichung eines rechtmäßigen Ziels ist, oder wenn es mehrere Mittel gibt, es das Mittel ist, welches am unwahrscheinlichsten die Menschenrechte verletzt. Der Nachweis der Begründung dieser Rechtfertigung in gerichtlichen sowie in Gesetzgebungsverfahren liegt beim Staat.

Angemessenheit: Jeder Fall der gesetzlich autorisierten Kommunikationsüberwachung muss geeignet sein, das spezifische legitime Ziel, welches festgelegt wurde, zu erfüllen.

Verhältnismäßigkeit: Kommunikationsüberwachung sollte als hochgradig invasive [oder: eindringende] Handlung angesehen werden, die in das Recht auf Privatsphäre und die Freiheit der Meinungsäußerung eingreift und die Grundlagen einer demokratischen Gesellschaft bedroht. Entscheidungen über Kommunikationsüberwachung müssen durch Abwägen der gesuchten Vorteile gegen die Schäden, die den Rechten des Einzelnen und anderen konkurrierenden Interessen zugefügt würden, getroffen werden, und sollten eine Betrachtung der Sensibilität der Informationen und der Schwere der Verletzung des Rechts auf Privatsphäre einbeziehen.

Dies erfordert insbesondere: Sollte ein Staat Zugang zu oder die Nutzung von geschützten Informationen anstreben, die durch Kommunikationsüberwachung im Rahmen einer strafrechtlichen Untersuchung gesammelt wurden, dann muss dies auf der zuständigen, unabhängigen und unparteiischen gerichtlichen Entscheidung begründet sein, dass:

- es eine hohe Wahrscheinlichkeit gibt, dass ein schweres Verbrechen begangen wurde oder begangen werden wird;
- der Beweis eines solchen Verbrechens durch den Zugriff auf die geschützten Daten erhalten werden würde;
- andere verfügbare und weniger invasive Ermittlungsmethoden ausgeschöpft sind;
- die abgerufenen Informationen in vernünftiger Weise auf diejenigen begrenzt werden, die für die mutmaßliche Straftat relevant sind, und jede weitere gesammelte Information sofort vernichtet oder zurückgegeben wird; und
- Informationen nur von der festgelegten Behörde abgerufen und nur für den Zweck, für den die Genehmigung erteilt wurde, verwendet werden.

Wenn der Staat mit Kommunikationsüberwachung Zugang zu geschützten Informationen zu einem Zweck erlangen will, der eine Person nicht der Strafverfolgung, Ermittlung, Diskriminierung oder Verletzung der Menschenrechte aussetzt, muss der Staat einer unabhängigen, unparteiischen und zuständigen Behörde Folgendes nachweisen:

- andere verfügbare und weniger invasive Ermittlungsmethoden wurden in Betracht gezogen;
- die abgerufenen Informationen werden in vernünftiger Weise auf die relevanten begrenzt und jede zusätzlich gesammelte Information wird sofort vernichtet oder dem betroffenen Individuum zurückgegeben; und
- Informationen werden nur von der festgelegten Behörde abgerufen und nur für den Zweck verwendet, für den die Genehmigung erteilt wurde.

Zuständige gerichtliche Behörden: Bestimmungen in Bezug auf die Kommunikationsüberwachung müssen von zuständigen gerichtlichen Behörden, die unparteiisch und unabhängig sind, festgelegt werden. Die Behörde muss:

- getrennt sein von der Behörde, welche die Kommunikationsüberwachung durchführt,
- vertraut sein mit den relevanten Themen und fähig sein, eine gerichtliche Entscheidung über die Rechtmäßigkeit der Kommunikationsüberwachung, die benutzte Technologie und Menschenrechte zu treffen, und
- über entsprechende Ressourcen verfügen, um die ihr übertragenen Aufgaben auszuführen.

Rechtsstaatliches Verfahren: Ein rechtsstaatliches Verfahren verlangt, dass Staaten die Menschenrechte jedes Einzelnen respektieren und garantieren, indem sie rechtmäßige Prozesse versichern, die jegliche Beeinträchtigung der Menschenrechte ordnungsgemäß und gesetzlich spezifiziert regeln, die konsistent durchgeführt werden, und die der allgemeinen Öffentlichkeit zugänglich sind. Insbesondere bei der Bestimmung seiner oder ihrer Menschenrechte hat jeder das Recht auf ein faires und öffentliches Verfahren innerhalb einer angemessenen Frist von einem unabhängigen, zuständigen und unparteiischen rechtmäßig gegründeten Gericht,(10) außer in Notfällen, wenn für Menschenleben Gefahr in Verzug ist. In solchen Fällen muss innerhalb einer vernünftigen und realisierbaren Frist eine rückwirkende Autorisierung eingeholt werden. Allein das Risiko der Flucht oder Zerstörung von Beweismitteln sollte niemals als ausreichend für eine rückwirkende Autorisierung angesehen werden.

Benachrichtigung des Nutzers: Personen sollten über die Entscheidung der Autorisierung einer Kommunikationsüberwachung informiert werden. Es sollten ausreichend Zeit und Informationen zur Verfügung gestellt werden, so dass die Person die Entscheidung anfechten kann. Des Weiteren sollte sie Zugang zu dem Material bekommen, welches für den Antrag der Autorisierung vorgelegt wurde. Eine Verzögerung der Benachrichtigung ist nur unter folgenden Bedingungen gerechtfertigt:

- Die Benachrichtigung würde den Zweck, für den die Überwachung genehmigt ist, ernsthaft gefährden oder es besteht eine unmittelbare Gefahr für Menschenleben, oder
- Die Erlaubnis einer Verzögerung der Benachrichtigung wird durch die zuständige Justizbehörde zum Zeitpunkt der Genehmigung der Überwachung erteilt; und
- Die betroffene Person wird benachrichtigt, sobald die Gefahr aufgehoben ist, oder innerhalb einer vernünftigen realisierbaren Frist; je nachdem, welches zuerst zutrifft, aber in jeden Fall zu dem Zeitpunkt, zu dem die Kommunikationsüberwachung abgeschlossen ist. Die Verpflichtung zur Benachrichtigung liegt beim Staat, aber in dem Fall, dass der Staat dem nicht nachkommt, sollten Kommunikationsdiensteanbieter die Freiheit haben, Personen über die Kommunikationsüberwachung freiwillig oder auf Anfrage zu benachrichtigen.

Transparenz: Staaten sollten bezüglich der Nutzung und des Umfangs der Techniken und Befugnisse der Kommunikationsüberwachung transparent sein. Sie sollten mindestens die gesammelten Informationen über die Anzahl der genehmigten und abgelehnten Anfragen, eine Aufschlüsselung der Anfragen nach Dienstanbieter und nach Ermittlungsart und -zweck veröffentlichen. Staaten sollten Personen genügend Informationen liefern, um zu gewährleisten, dass sie den Umfang, die Art und Anwendung der Gesetze,

welche die Kommunikationsüberwachung erlauben, zu verstehen. Staaten sollten Diensteanbieter befähigen, die von ihnen angewendeten Prozesse zu veröffentlichen, wenn sie staatliche Kommunikationsüberwachung bearbeiten, an diesen Prozessen festzuhalten und Berichte der staatlichen Kommunikationsüberwachung zu veröffentlichen.

Öffentliche Aufsicht: Staaten sollten unabhängige Aufsichtsmechanismen schaffen, die Transparenz und Verantwortung der Kommunikationsüberwachung gewährleisten.(11) Aufsichtsmechanismen sollten die Befugnis haben, auf alle potenziell relevanten Informationen über staatliche Maßnahmen, wenn notwendig auch auf geheime oder als Verschlusssachen gekennzeichnete Informationen, zuzugreifen; zu beurteilen, ob der Staat seine rechtmäßigen Fähigkeiten legitim nutzt; zu beurteilen, ob der Staat die Informationen über den Einsatz und den Umfang der Techniken und Befugnisse der Kommunikationsüberwachung transparent und genau veröffentlicht hat; und regelmäßige Berichte und andere für die Kommunikationsüberwachung relevante Informationen zu veröffentlichen. Unabhängige Kontrollmechanismen sollten in Ergänzung zur Aufsicht geschaffen werden, die bereits über einen anderen Teil der Regierung zur Verfügung steht.

Integrität der Kommunikation und der Systeme: Um die Integrität, Sicherheit und Privatsphäre der Kommunikationssysteme zu gewährleisten, und in Anerkennung der Tatsache, dass Abstriche bei der Sicherheit für staatliche Zwecke fast immer die Sicherheit im Allgemeinen infrage stellen, sollten Staaten die Dienstleister oder Hardware- oder Softwarehändler nicht zwingen, Überwachungs- oder Beobachtungsfunktionen in ihre Systeme einzubauen oder bestimmte Informationen lediglich für Zwecke der staatlichen Überwachung zu sammeln oder zu speichern. A priori Vorratsdatenspeicherung oder Sammlung sollte nie von Dienstleistern gefordert werden. Personen haben das Recht, sich anonym zu äußern; Staaten sollten daher auf die zwingende Identifizierung der Nutzer als Voraussetzung für die Leistungserbringung verzichten.(12)

Schutzmaßnahmen für die internationale Zusammenarbeit: Als Reaktion auf die Veränderungen der Informationsflüsse und Kommunikationstechnologien und -dienstleistungen, kann es notwendig sein, dass Staaten Hilfe von einem ausländischen Dienstleister anfordern. Dementsprechend sollten die gemeinsamen Rechtshilfeverträge und andere Vereinbarungen, die von den Staaten eingegangen wurden, sicherstellen, dass in Fällen, in denen die Gesetze mehr als eines Staates für die Kommunikationsüberwachung angewendet werden können, derjenige verfügbare Standard mit dem höheren Schutzniveau für den Einzelnen angewendet wird. Wo Staaten Unterstützung für Zwecke der Strafverfolgung suchen, sollte der Grundsatz der beiderseitigen Strafbarkeit angewendet werden. Staaten dürfen gemeinsame Rechtshilfeprozesse und ausländische Anfragen nach geschützten Informationen nicht nutzen, um inländische gesetzliche Beschränkungen der Kommunikationsüberwachung zu umgehen. Gemeinsame Rechtshilfeprozesse und andere Vereinbarungen sollten klar dokumentiert werden, öffentlich zugänglich sein und dem Schutz des fairen Verfahrens unterliegen.

Schutzmaßnahmen gegen unrechtmäßigen Zugang: Die Staaten sollten Gesetze erlassen, welche illegale Kommunikationsüberwachung durch öffentliche oder private Akteure kriminalisieren. Die Gesetze sollten ausreichende und erhebliche zivil-und strafrechtliche Sanktionen, Schutz für Whistleblower und Wege für die Wiedergutmachung von Betroffenen enthalten. Die Gesetze sollten vorsehen, dass alle Informationen, welche in einer Weise gesammelt wurden, die mit diesen Grundsätzen unvereinbar ist, in einem Verfahren als Beweise unzulässig sind, genauso wie Beweise, die von solchen Informationen abgeleitet sind. Die Staaten sollten außerdem Gesetze erlassen mit der Maßgabe, dass das Material zerstört oder der Person zurückgegeben werden muss, nachdem das durch Kommunikationsüberwachung gesammelte Material zu dem Zweck genutzt wurde, zu welchem es bereitgestellt wurde.

Die Erklärung kann über die Webseite https://www.necessaryandproportionate.org/ unterstützt werden. Die

vorliegende Übersetzung wurde von Digitalcourage e.V. erstellt.

Anmerkungen:

(1) Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

(2) Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

(3) Communications metadata may include information about our identities (subscriber information, device information), interactions (origins and destinations of communications, especially those showing websites visited, books and other materials read, people interacted with, friends, family, acquaintances, searches conducted, resources used), and location (places and times, proximities to others); in sum, metadata provides a window into nearly every action in modern life, our mental states, interests, intentions, and our innermost thoughts.

(4) For example, in the United Kingdom alone, there are now approximately 500,000 requests for communications metadata every year, currently under a self-authorising regime for law enforcement agencies who are able to authorise their own requests for access to information held by service providers. Meanwhile, data provided by Google's Transparency reports shows that requests for user data from the U.S. alone rose from 8888 in 2010 to 12,271 in 2011. In Korea, there were about 6 million subscriber/poster information requests every year and about 30 million requests for other forms of communications metadata every year in 2011-2012, almost of all of which were granted and executed. 2012 data available at http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=3
.

(5) See as examples, a review of Sandy Petland's work, 'Reality Mining', in MIT's Technology Review, 2008, available at http://www2.technologyreview.com/article/409598/tr10-reality-mining/ and also see Alberto Escudero-Pascual and Gus Hosein, 'Questioning lawful access to traffic data', Communications of the ACM, Volume 47 Issue 3, March 2004, pages 77 - 82.

(6) Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, May 16 2011, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

(7) "People disclose the phone numbers that they dial or text to their cellular providers, the URLS that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers ... I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled

to Fourth Amendment protection." United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

(8) "Short-term monitoring of a person’s movements on public streets accords with expectations of privacy" but "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." United States v. Jones, 565 U.S., 132 S. Ct. 945, 964 (2012) (Alito, J. concurring).

(9) "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.* A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts." U.S. v. Maynard, 615 F.3d 544 (U.S., D.C. Circ., C.A.)p. 562; U.S. v. Jones, 565 U.S. __, (2012), Alito, J., concurring. "Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past…In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of 'private life' for the purposes of Article 8(1) of the Convention." (Rotaru v. Romania, [2000] ECHR 28341/95, paras. 43-44.)

(10) The term "due process" can be used interchangeably with "procedural fairness" and "natural justice", and is well articulated in the European Convention for Human Rights Article 6(1) and Article 8 of the American Convention on Human Rights.

(11) The UK Interception of Communications Commissioner is an example of such an independent oversight mechanism. The ICO publishes a report that includes some aggregate data but it does not provide sufficient data to scrutinise the types of requests, the extent of each access request, the purpose of the requests, and the scrutiny applied to them. See http://www.iocco-uk.info/sections.asp?sectionID=2&type=top .

(12) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27, para 84.
