Foro: Comisión de Política Especial y Descolonización

Tema #13-02: Evaluación del creciente avance e implementación de sistemas de vigilancia masiva por parte de los gobiernos mundiales

Oficial Estudiantil: Camilo Dugand

Posición: Moderador de la Comisión de Política Especial y Descolonización

---

Introducción

Con los avances tecnológicos del siglo 21, la expansión del Internet y la facilidad de comunicación global e instantánea que este ofrece, se ha vuelto muchísimo más sencilla la transmisión de información por todo el mundo. Como consecuencia de esto, se ha ampliado la capacidad operacional de redes terroristas, narcotraficantes, mafias y otros grupos de crimen organizado. Los gobiernos mundiales han tratado de combatir a estas redes criminales utilizando diferentes métodos, uno de los más notables y controversiales siendo la vigilancia masiva.

De la misma manera en la que la tecnología facilita la comunicación global, también se ha vuelto mucho más avanzada la manera en la que la información puede ser interceptada y descifrada. Gobiernos como el de Estados Unidos, Alemania, Rusia y China ya tienen implementados sistemas de interceptación de información a nivel global. El modus operandi de estos sistemas, a pesar de ser bastante sofisticado y complejo, les permite a estos gobiernos interceptar desde llamadas telefónicas en las Filipinas a mensajes de texto en Nicaragua sin restricciones. Cada vez que alguien en cualquier parte del mundo se comunica con otra persona a través de medios digitales, la información enviada y recibida viaja instantáneamente a un servidor que puede estar al otro lado del mundo. De esta manera, la información es retenida en el servidor y es asequible y accesible al dueño del servidor, o a terceros con acceso a los servidores.

La vigilancia masiva, desde un punto de vista legal, depende de las leyes de cada país. En muchos países, la interceptación de comunicaciones hacia una persona es permitida solamente bajo una orden judicial otorgada por un juez. En otros, como es el caso de Francia, la autorización judicial no es necesaria para que el estado haga este tipo de acciones.

La controversia del asunto de la vigilancia masiva es evidente. Los activistas de derechos humanos afirman que se está violando el derecho humano a la privacidad cuando los gobiernos tienen la capacidad y autoridad de interceptar constantemente las comunicaciones de cualquier ser humano, sea ciudadano de ese país o no. Por esta razón, existe gran oposición a los sistemas implementados, además de cierta creencia popular que la regularización de la vigilancia masiva sería un paso enorme hacia un mundo distópico que se asemeja al presentado por George Orwell en su novela "1984."

Definición de Términos

Vigilancia masiva

Según Amnistía Internacional, "La vigilancia masiva indiscriminada es el control de las comunicaciones por Internet y telefónicas de un gran número de personas –a veces de países enteros– sin que existan indicios suficientes de conducta delictiva. Este tipo de vigilancia no es legal."

Artículo 12 de la Declaración Universal de los Derechos Humanos

El artículo 12 de la Declaración Universal de los Derechos Humanos (DUDH) destaca que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques." Por ende y por definición, la vigilancia masiva viola directamente este derecho humano.

Whistleblower (Informante)

Según el diccionario Merriam-Webster, un informante o *whistleblower*, como se conoce en inglés, es "alguien que revela algo encubierto o que informa contra otro." Un *whistleblower*, por lo general, revela información al público que él o ella considera evidencia de actos ilícitos cometidos por un gobierno

u organización. Algunas figuras notorias como Edward Snowden y Julian Assange han filtrado información acerca de los sistemas de vigilancia masiva implementados por los gobiernos, y por lo tanto son perseguidos y han encontrado asilo en otros países.

WikiLeaks

En el 2006, Julian Assange, un genio informático previamente acusado de hackear el Departamento de Defensa de los Estados Unidos, fundó la página web WikiLeaks. WikiLeaks funciona como una plataforma en donde *whistleblowers* en cualquier lugar del mundo pueden filtrar documentos e información de manera completamente anónima. Por medio de WikiLeaks, el público ha obtenido gran cantidad de información sobre las operaciones y sistemas de vigilancia masiva por parte de gobiernos como el de Estados Unidos y Alemania.

Los Cinco Ojos

Los "Cinco Ojos" es "una alianza de intercambio de información formada por Australia, Canadá, Estados Unidos, Nueva Zelanda y Reino Unido. La Alianza de los Cinco Ojos tiene su origen en la colaboración en inteligencia de Reino Unido y Estados Unidos durante la Segunda Guerra Mundial," según Amnistía Internacional. Organizaciones como los "Cinco Ojos," a pesar de ser coaliciones de naciones como las Naciones Unidas, trabajan para un fin legal como es la seguridad pero con estrategias que están al margen de la ley, como es el caso de la vigilancia masiva.

Servicio de inteligencia

Según el Centro Nacional de Inteligencia de España, los servicios de inteligencia "son organismos del Estado que tienen como misión obtener información, no alcanzable por otros organismos, y difundir inteligencia sobre diversas amenazas, a fin de hacer posible su prevención y facilitar la toma de decisiones por el Gobierno." Servicios de inteligencia como la Agencia de Seguridad Nacional de Estados Unidos (NSA) y la Jefatura de Comunicaciones del Gobierno del Reino Unido (GCHQ) son protagonistas en cuanto a sistemas de vigilancia masiva, y mantienen la mayoría de sus operaciones de manera clasificada.

Metadatos

El término metadatos se usa para referirse a la "data acerca de otra data." Cuando se envía información de manera digital, existe mucha información acerca de esta comunicación además del

contenido del mensaje. Los metadatos consisten de información como la localización desde donde se envió el mensaje y la localización de donde fue recibido, qué tipo de dispositivo lo envió y que tipo de dispositivo lo recibió, a qué hora fue enviado y a qué hora fue recibido, la duración de la comunicación y la información del emisor y el recipiente, como correo electrónico, teléfono, etc. Para defender su argumento de que no se invade la privacidad, los servicios de inteligencia que utilizan sistemas de vigilancia masiva alegan que solo tienen acceso a la metadatos y no al contenido del mensaje en sí. Sin embargo, hay quienes sostienen que de la metadatos se puede obtener una imagen muy completa de la persona y por ende sí se está violando el derecho fundamental a la privacidad al obtener estos datos.

Guía General

Creciente espionaje y vigilancia

Vigilancia Interna

La vigilancia masiva que ejercen los países con estos sistemas es utilizada para vigilar a los ciudadanos mismos de ese país. En Estados Unidos, la NSA utiliza varios programas como Prism, Upstream y Mystic para la recopilación de los datos electrónicos de todas las comunicaciones dentro de su territorio. Estos programas utilizan la cooperación de compañías de comunicación como Google, Yahoo y Verizon para obtener todos los datos de la comunicación e información del usuario. En China, se conoce que el gobierno monitorea todas las actividades de Internet dentro de su país y todas la llamadas telefónicas, y con esta información puede perseguir a disidentes políticos.

Espionaje Externo

Además de vigilar a sus ciudadanos, los gobiernos también utilizan los sistemas de vigilancia masiva para espiar a personas en el extranjero. Bajo la Ley de Vigilancia de Inteligencia Extranjera (FISA) de 1978, la NSA ha utilizado sus sistemas para espiar a personas que no son ciudadanos estadounidenses. Según una fuente de WikiLeaks, el gobierno de Estados Unidos estuvo interceptando las llamadas telefónicas de la canciller alemana Angela Merkel y sus asesores más cercanos. Esta filtración creó una tensión entre estos dos países. De la misma forma, el Servicio Federal de Inteligencia de Alemania (BND) también fue acusado recientemente de utilizar sistemas de vigilancia para espiar a funcionarios de la Casa Blanca y el Departamento del Tesoro. Con los avanzados sistemas que utilizan ambos gobiernos para espiarse entre sí, vigilan también a personas en todo el mundo.

Sistemas de vigilancia masiva

La NSA de Estados Unidos utiliza un sistema de vigilancia masiva que está compuesto de programas como XKeyscore, Prism, Upstream, y Mystic. XKeyscore es un programa utilizado para recolectar datos del tráfico de internet, contenido de mensajes texto, correos electrónicos, y los metadatos de las llamadas telefónicas. Prism es el programa que utiliza la NSA para extraer información de los servidores de colaboradores como Google, Yahoo y Facebook. Con Upstream, la NSA puede extraer información mientras viaja de servidor a servidor por Internet, y con Mystic pueden obtener los metadatos de llamadas telefónicas y el contenido de las llamadas en ciertos países como las Bahamas.

Junto con la GCHQ del gobierno británico, la NSA también creó los programas Tempora y MUSCULAR. Con Tempora, ambos gobiernos pueden obtener directamente la información transmitida por cables de fibra óptica y con MUSCULAR pueden interceptar y recopilar información de los servidores de Google Y Yahoo, sin su permiso. La gran variedad de sistemas existentes le facilita a los gobiernos vigilar de manera constante y sencilla las comunicaciones de ciudadanos por todo el mundo.

Acciones legislativas

La cuarta enmienda de la Constitución de los Estados Unidos destaca que “el derecho del pueblo a la seguridad en sus personas, domicilios, papeles y efectos, contra registros y detenciones arbitrarias, será inviolable...” El derecho a no ser registrado de ninguna forma sin una orden judicial es un concepto establecido en las leyes de muchos países del mundo.

Fomentando la vigilancia masiva

Utilizando medidas legislativas, países como Estados Unidos, Francia y Alemania “legalizan” ante su sistema judicial el uso de sistemas de vigilancia masiva. En Estados Unidos, la ley FISA, en la sección 720 describe que se “permite la recolección masiva de datos” por parte de los servicios de inteligencia. En el 2015, expiró este decreto, mas la NSA todavía puede recolectar datos de esta manera por medio de una orden judicial de las cortes FISA. También, bajo la Orden Ejecutiva 12333, la NSA tiene autorización legal de acceder a los servidores de las compañías de comunicación y extraer datos de los usuarios. Y bajo la Ley Patriótica, sección 215, la NSA puede acceder a los metadatos de las llamadas telefónicas sin restricciones legales.

En Alemania, la Corte Constitucional pasó en Junio de 2017 una ley que permite a las organizaciones policiacas hackear los teléfonos móviles de los ciudadanos alemanes e instalar *malwares*,

o programas que les permitan monitorear, en vivo y en directo, todas las actividades del dueño del teléfono móvil.

En contra de la vigilancia masiva

Existen países que se adhieren a las leyes internacionales con respecto al uso de sistemas de vigilancia masiva. En Colombia, "dos artículos del Código de Extinción de Dominio que facultaba a la Fiscalía para hacer interceptaciones telefónicas sin que mediara una orden judicial fueron declarados inexequibles por la Corte Constitucional." En países como Islandia, en donde se establece la Ley de Protección de Datos, o Dinamarca, en donde se siguen estableciendo leyes de privacidad rigurosas, las leyes de vigilancia se basan en la protección del derecho humano a la privacidad.

Filtraciones sobre la vigilancia masiva

NSA Files

En el año 2013, un entonces analista de la NSA llamado Edward Snowden filtró documentos de la agencia de inteligencia con los detalles de los mecanismos que la NSA utiliza para vigilar a sus ciudadanos y a personas de todo el mundo. En los documentos se encuentran los detalles de los programas XKeyscore, Prism, Mystic y Tempora. Gracias a esta filtración, la controversia de la vigilancia masiva se llegó a conocer en cada esquina del planeta y se abrió el debate acerca de cuál es el rol de la población frente a este tema.

Spy Files

A partir del 2011 y hasta el 2014, WikiLeaks publicó una serie de cuatro sets de documentos sobre los sistemas de vigilancia masiva. En el cuarto set de documentos se habla de FinFisher, una compañía alemana con el propósito de producir tecnología de vigilancia y *malware* para poder infiltrarse en computadoras con sistemas operativos Windows, OS X y Linux, al igual que teléfonos móvil con sistemas iOS, Android, BlackBerry y Windows Mobile. Se alega que esta compañía alemana vende sus dispositivos a los regímenes con más demanda a la vigilancia masiva.

BND - NSA Files

El 1 de diciembre de 2016 WikiLeaks publicó un total de 90 gigabytes en documentos sobre la colaboración entre la BND y la NSA en relación a la vigilancia masiva. Los 2 420 documentos revelan datos importantes acerca de las operaciones conjuntas de las dos agencias de seguridad. La NSA utilizó

sus bases aliadas en Alemania para espiar a los ciudadanos alemanes, y la BND lograba vigilar las operaciones de compañías americanas en territorio Alemán. Incluso, uno de los documentos describe como a un empleado de la BND se le encarga la redacción e instalación de un software para el programa XKeyscore de la NSA.

Vault 7

En marzo de 2017, WikiLeaks empezó a publicar documentos acerca de las operaciones de vigilancia de la Agencia Central de Inteligencia (CIA). Con el título de "Vault 7," se han revelado varios documentos detallando los métodos de operaciones de la CIA, mencionando proyectos como Dark Matter, Grasshopper, HIVE, Archimedes, Athena, CouchPotato y Dumbo, utilizados en conjunto para interceptar y corromper dispositivos electrónicos y monitorearlos. Hasta la fecha, se han publicado incluso más documentos que en los NSA Files, y según Julian Assange esta filtración es más grande que la de Snowden en 2013.

Objetivos de la vigilancia masiva

Las agencias de seguridad como la BND, GCHQ y NSA sostienen que el objetivo principal de la vigilancia masiva es mantener a sus ciudadanos seguros y evitar cualquier tipo de ataques a la sociedad. Por medio de los sistemas previamente mencionados, estos servicios de inteligencia tienen la capacidad de advertir actos de terrorismo y crimen organizado. Después de los ataques del 11 de septiembre de 2001 y los atentados terroristas por parte del Estado Islámico de Irak y Siria (ISIS) en Francia, Alemania, España, Turquía y otros países en Europa, estos gobiernos se sienten presionados a incrementar los niveles de seguridad dentro de sus territorios y acuden a utilizar la vigilancia masiva.

Oposición a la vigilancia

El mayor argumento de la oposición a la vigilancia masiva es el de defender el derecho humano a la privacidad. Los programas utilizados por agencias como la NSA recopilan absolutamente todos los datos digitales de la vida personal de los ciudadanos, sean terroristas o no. Y aunque las agencias de seguridad alegan que no acceden jamás a esta información, siempre tendrán acceso a ella. La información que se obtiene por medio de estos sistemas puede ser utilizada para extorsionar a opositores políticos o a las minorías en un país. Los sistemas de vigilancia y espionaje masivo, sin importar el supuesto fin que tengan, pueden ser potencialmente utilizados para controlar a los ciudadanos de un país, región, continente o inclusive el mundo entero. Con este miedo a un "ojo que todo lo ve" o *Big Brother* de la

novela 1984, los opositores a la vigilancia masiva sostienen que la privacidad es un derecho fundamental que no puede ser violado en una sociedad libre.

Países y Organizaciones Involucrados:

Estados Unidos de America

El gobierno estadounidense es uno de los que más invaden la privacidad de los ciudadanos y extranjeros con sus sistemas de vigilancia masiva. Gracias a las revelaciones de Snowden, se sabe cómo opera la NSA cuando espía a las personas alrededor del mundo. El gobierno de Estados Unidos es muy permisivo con respecto a cómo los sistemas de vigilancia masiva operan en relación a la información transmitida por medios digitales. Leyes como la Ley Patriótica, la Ley FISA y la Orden Ejecutiva 12333 son interpretadas por la NSA, la CIA y el FBI como permisos legales para violar el derecho a la privacidad con los sistemas de vigilancia masiva. De esta forma, el gobierno estadounidense sigue espiando a personas en todas partes del mundo sin restricciones o consecuencias.

Alemania

Alemania, a pesar de en repetidas ocasiones rechazar la vigilancia masiva, utiliza también estos sistemas con cooperación del gobierno de Estados Unidos. Debido a los recientes ataques terroristas hacia la población alemana, se han pasado leyes que permiten de manera mucho más extensa el uso de la vigilancia masiva como medio para interceptar las comunicaciones entre células terroristas. Sin embargo, todavía existe el dilema de la violación al derecho humano de la privacidad y organizaciones como WikiLeaks se enfocan en difamar las políticas del gobierno alemán con el fin de defender este derecho fundamental.

Reino Unido

Con la ayuda de Estados Unidos, el Reino Unido se ha convertido en uno de los países con mayor vigilancia en el mundo. La extensa red de cámaras de seguridad, combinada con el uso de tecnología digital para interceptar comunicaciones le ha permitido al gobierno británico vigilar a sus ciudadanos y a los del resto del planeta. El programa Tempora, que desarrolló con ayuda americana, es utilizado a lo largo de su territorio y más allá de él para recopilar los datos electrónicos de personas alrededor del mundo. Como miembro de la coalición de los Cinco Ojos, el Reino Unido mantiene alianzas informáticas con las agencias de seguridad de los Estados Unidos.

China

De los países con mayor vigilancia masiva, China es uno de los más aferrados a las políticas de vigilancia invasiva. Bajo un régimen en donde la censura es regularizada, la libertad de prensa, opinión y circulación es casi inexistente. El uso del Internet es restringido, y sitios web como Google son prohibidos por ley. Además de eso, las comunicaciones son totalmente monitoreadas, e inclusive el uso de lenguaje que pueda oponerse a la posición del gobierno es fácilmente rastreado por el estado y es motivo de encarcelamiento. Comparado con Estados Unidos, Alemania y el Reino Unido, China es sin lugar a dudas el país con más vigilancia masiva y con las mayores violaciones a los derechos humanos de privacidad y libertad.

Islandia

En Islandia se está creando el mayor refugio a los derechos de libertad de opinión y privacidad. Con el establecimiento de fuertes leyes que protegen la privacidad y los datos, Islandia se ha convertido en una superpotencia a nivel de derechos humanos. Desde la filtración de Snowden en 2013, las empresas privadas buscan dónde instalar de manera segura sus servidores para proteger sus datos. Islandia se ha convertido en el lugar más atractivo. El objetivo de esta política anti-vigilancia masiva es proteger y preservar la privacidad y obstaculizar los canales de espionaje mundiales hasta el punto que se vuelva inviable la vigilancia masiva.

Dinamarca

Como en Islandia, Dinamarca también se ha unido a la causa para proteger el derecho a la privacidad. Datatilsynet, la agencia de protección de datos de Dinamarca, es la encargada de supervisar a las compañías privadas y al gobierno para asegurarse de que sus métodos de inteligencia cumplan con las leyes internacionales en términos de derechos humanos. De esta manera, el estado danés se asegura de no quebrantar ninguna ley internacional con relación a la privacidad.

Suecia

El gobierno sueco, junto con sus aliados, se mantiene dentro del margen de la ley con respecto al derecho fundamental a la privacidad del ser humano. Como en Dinamarca, la Ley de Protección de Datos mantiene al gobierno y otras organizaciones locales supervisadas en materia de protección a la privacidad al obtener inteligencia. La ley prohíbe la interceptación sistemática y masiva de comunicaciones, y

solamente con orden judicial puede el gobierno vigilar a un individuo.

Línea de Tiempo

Fecha	Descripción del evento
1919	El Departamento de Estado de Estados Unidos autoriza la creación de el "Cipher Bureau" o Oficina del Cifrado, que sería el predecesor a la NSA.
1945	Estados Unidos crea SHAMROCK, un proyecto para interceptar todos los datos telegráficos que entran y salen del territorio estadounidense.
1952	El presidente de Estados Unidos Harry Truman autoriza una directiva para crear la Agencia Nacional de Seguridad
1972	La Corte Suprema de Estados Unidos sentencia que la Cuarta Enmienda de la Constitución, que protege a los ciudadanos de ser registrados sin causa, aplica a casos de vigilancia electrónica y una orden judicial es necesaria.
1978	El Congreso estadounidense aprueba la Ley de Vigilancia de Inteligencia Extranjera (FISA), y el establecimiento de cortes FISA que aprueben los casos de vigilancia doméstica.
Septiembre 2001	Al-Qaeda ataca territorio estadounidense al secuestrar aviones comerciales y estrellarlos contra los edificios del World Trade Center en Nueva York y las oficinas del Departamento de Defensa en Washington D.C.
Octubre 2001	El Congreso de Estados Unidos aprueba la Ley Patriótica.
Diciembre 2006	El hacker Julian Assange funda WikiLeaks, con el propósito de atraer a whistleblowers a dar información de manera anónima.
Diciembre 2011	WikiLeaks empieza a revelar los Spy Files.
Enero 2013	Edward Snowden filtra los documentos clasificados de la NSA que describen detalladamente las operaciones de vigilancia masiva de la agencia.
Junio 2015	El Congreso de Estados Unidos aprueba la Ley de la Libertad, que reemplaza y modifica la Ley Patriótica.
Diciembre 2016	WikiLeaks publica los BND-NSA Files.
Marzo 2017	WikiLeaks revela operaciones de espionaje de la CIA en los "Vault 7" Files.

Implicación de la O.N.U, resoluciones relevantes, tratados y acontecimientos

La Organización de las Naciones Unidas ha tomado en sus manos el importante tema de la vigilancia masiva en el Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH). El 26 de marzo de 2015, en Ginebra el Consejo de Derechos Humanos decidió aprobar por consenso la resolución L.27 denominada "El derecho a la privacidad en la era digital," presentada por Brasil, Alemania y México." Esta resolución reitera lo ya establecido por el artículo 12 de la Declaración Universal de los Derechos Humanos. Sin embargo, la vigilancia masiva sigue creciendo y las naciones que la utilizan hacen caso omiso a esta resolución.

Evaluación de los intentos previos para resolver la situación

Con la resolución L.27 del ACNUDH solamente se recuerda a los países miembros de la ONU que existe ya una ley internacional y un derecho humano que prohíbe el uso de sistemas de vigilancia invasivos y masivos. Los países que más utilizan estos sistemas como Estados Unidos, el Reino Unido, China y Alemania siguen pasando leyes para facilitar el uso de estos sistemas dentro del rango legal, más no cumplen con las leyes internacionales establecidas por la ONU. Por esta razón, la resolución pasada no tuvo el efecto deseado.

Posibles Soluciones

Con la resolución pasada por el ACNUDH, no se llegó a una verdadera solución al problema de la vigilancia masiva. Se necesita una resolución que establezca unos parámetros fijos y mandatorios para todas las naciones que utilizan sistemas de vigilancia masiva. El propósito de esta nueva resolución no sería aprobar o prohibir el uso de estos sistemas, sino implementar una regularización efectiva, constante y minuciosa para mantener a estos programas dentro del margen legal internacional. La diferencia de esta nueva resolución con respecto a la L.27 del ACNUDH es que se estaría tocando el tema no desde un punto de vista estrictamente de derechos humanos sino de política y ley internacional, lo cual ayudaría a establecer la resolución como un decreto y no simplemente una exhortación. De esta forma, con un método de regulación eficaz, la vigilancia masiva podría ser manejada con mayor cuidado y para la protección de los derechos fundamentales de la humanidad.

Bibliografía

Bejerano, Pablo G. "Islandia quiere ser la Suiza de los datos." *Eldiario.es*, Eldiario.es, 9 Jan. 2015, www.eldiario.es/turing/islandia-privacidad-datos_0_343666334.html. Accessed 6 Sept. 2017.

Berlin, Reuters in. "NSA tapped German Chancellery for decades, WikiLeaks claims." *The Guardian*, Guardian News and Media, 8 July 2015, www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel. Accessed 6 Sept. 2017.

"CNI-Centro Nacional de Inteligencia." *CNI - Centro Nacional de Inteligencia - ¿Qué es un servicio de inteligencia?*, CNI, www.cni.es/es/preguntasfrecuentes/pregunta_001.html?pageIndex=1&faq=si&size=15. Accessed 6 Sept. 2017.

Debenedetti;, Gabriel. "Factbox: History of mass surveillance in the United States." *Reuters*, Thomson Reuters, 7 June 2013, www.reuters.com/article/us-usa-security-records-factbox/factbox-history-of-mass-surveillance-in-the-united-states-idUSBRE95617O20130607. Accessed 6 Sept. 2017.

España, Amnistía Internacional. "Infórmate sobre vigilancia masiva." *En Internet*, Amnistia Internacional, 11 Apr. 2017, www.es.amnesty.org/en-que-estamos/temas/vigilancia-masiva/. Accessed 6 Sept. 2017.

"FISA 702." *U.S. House of Representatives Permanent Select Committee on Intelligence*, U.S. House of Representatives Permanent Select Committee on Intelligence, intelligence.house.gov/fisa-702/. Accessed 6 Sept. 2017.

LastWeekTonight. "Government Surveillance: Last Week Tonight with John Oliver (HBO)." *YouTube*, HBO, 5 Apr. 2015, www.youtube.com/watch?v=XEVlyP4_11M. Accessed 6 Sept. 2017.

Greenwald, Glenn. "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'." *The Guardian*, Guardian News and Media, 31 July 2013, www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. Accessed 6 Sept. 2017.

Griffin, Andrew. "WikiLeaks publishes massive trove of CIA spying files in 'Vault 7' release." *The Independent*, Independent Digital News and Media, 8 Mar. 2017,

www.independent.co.uk/life-style/gadgets-and-tech/news/wikileaks-cia-vault-7-julian-assange-year-zero-documents-download-spying-secrets-a7616031.html. Accessed 6 Sept. 2017.

TestTubeNetwork. "How Invasive Is China's Mass Surveillance?" *YouTube*, YouTube, 14 Oct. 2015, www.youtube.com/watch?v=_eAxY2Trfqk. Accessed 6 Sept. 2017.

Huggler, Justin. "German intelligence accused of spying on USA." *The Telegraph*, Telegraph Media Group, 22 June 2017, www.telegraph.co.uk/news/2017/06/22/germany-accused-hypocrisy-claims-spied-usa/. Accessed 6 Sept. 2017.

"International Comparative Legal Guides." *Data Protection 2017 | Laws and Regulations | Sweden | ICLG*, Global Legal Group, iclg.com/practice-areas/data-protection/data-protection-2017/sweden. Accessed 6 Sept. 2017.

"Introduction to the Danish Data Protection Agency." *Datatilsynet*, Datatilsynet, www.datatilsynet.dk/english/the-danish-data-protection-agency/introduction-to-the-danish-data-protection-agency/. Accessed 6 Sept. 2017.

Khazan, Olga. "Actually, Most Countries Are Increasingly Spying on Their Citizens, the UN Says." *The Atlantic*, Atlantic Media Company, 6 June 2013, www.theatlantic.com/international/archive/2013/06/actually-most-countries-are-increasingly-spying-on-their-citizens-the-un-says/276614/. Accessed 6 Sept. 2017.

"La Declaración Universal de Derechos Humanos | Naciones Unidas." *United Nations*, United Nations, www.un.org/es/universal-declaration-human-rights/. Accessed 6 Sept. 2017.

MacAskill, Ewen, et al. "NSA files decoded: Edward Snowden's surveillance revelations explained." *The Guardian*, Guardian News and Media, 1 Nov. 2013, www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. Accessed 6 Sept. 2017.

"NSA Ends Bulk Collection of Telephony Metadata under Section 215." *Lawfare*, Lawfare, 2 Dec. 2015, www.lawfareblog.com/nsa-ends-bulk-collection-telephony-metadata-under-section-215. Accessed 6 Sept. 2017.

"ONU crea Relator Especial sobre el derecho a la privacidad en la era digital |." *Panorama*, Panorama, 27 Mar. 2015,

panorama.ridh.org/onu-crea-relator-especial-sobre-el-derecho-a-la-privacidad-en-la-era-digital/. Accessed 6 Sept. 2017.

PAÍS, EL. "Bajo la vigilancia de los Cinco Ojos." *EL PAÍS*, EL PAÍS, 6 July 2013, elpais.com/internacional/2013/07/05/actualidad/1373038892_139217.html. Accessed 6 Sept. 2017.

PAÍS, EL. "¿Cómo legislan los Gobiernos sobre vigilancia masiva?" *EL PAÍS*, Síguenos en Síguenos en Twitter Síguenos en Facebook Síguenos en Twitter Síguenos en Instagram, 5 June 2015, elpais.com/internacional/2015/06/05/actualidad/1433515872_277281.html. Accessed 6 Sept. 2017.

"Fiscalía no puede interceptar sin orden judicial: Corte Constitucional." *El Tiempo*, El Tiempo, 13 Aug. 2015, www.eltiempo.com/archivo/documento/CMS-16226616. Accessed 6 Sept. 2017.

"Privacy International." *Metadata*, Privacy International, www.privacyinternational.org/node/53. Accessed 6 Sept. 2017.

"Privacy International." *United Nations adopts resolution condemning unlawful government surveillance*, Privacy International, 25 Nov. 2014, www.privacyinternational.org/node/402. Accessed 6 Sept. 2017.

"Revealed: the obscure legal authority the NSA is using to spy on millions, and how to stop it." *EFF Action Center*, EFF Action Center, act.eff.org/action/tell-obama-stop-mass-surveillance-under-executive-order-12333. Accessed 6 Sept. 2017.

"Sección Argentina de Amnistía Internacional | Trabajamos para defender los Derechos Humanos en el Mundo." *En todo el mundo se rechaza la vigilancia masiva de Estados Unidos*, Amnistia Internacional, amnistia.org.ar/en-todo-el-mundo-se-rechaza-la-vigilancia-masiva-de-estados-unidos/. Accessed 6 Sept. 2017.

"Surveillance Under the Patriot Act." *American Civil Liberties Union*, American Civil Liberties Union, www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act. Accessed 6 Sept. 2017.

"The Data Protection Act." *Persónuvernd. Þínar upplýsingar, þitt einkalíf.*, Persónuvernd, www.personuvernd.is/information-in-english/greinar/nr/438. Accessed 6 Sept. 2017.

"Timeline: U.S. Spying and Surveillance." *Infoplease*, Infoplease, www.infoplease.com/us/timeline-us-spying-and-surveillance. Accessed 6 Sept. 2017.

Welle, Deutsche. "New surveillance law: German police allowed to hack smartphones | Germany | DW | 22.06.2017." *DW.COM*, DW, www.dw.com/en/new-surveillance-law-german-police-allowed-to-hack-smartphones/a-39372085. Accessed 6 Sept. 2017.

Welle, Deutsche. "Things to know about Germany's recent surveillance laws | Germany | DW | 26.06.2017." *DW.COM*, DW, www.dw.com/en/things-to-know-about-germanys-recent-surveillance-laws/a-39421060. Accessed 6 Sept. 2017.

"What is XKeyscore? - Definition from WhatIs.Com." *WhatIs.com*, What Is, whatis.techtarget.com/definition/XKeyscore. Accessed 6 Sept. 2017.

"Whistle-Blower." *Merriam-Webster*, Merriam-Webster, www.merriam-webster.com/dictionary/whistle-blower. Accessed 6 Sept. 2017.

Yan, Holly. "What is the FISA court, and why is it so secretive?" *CNN*, Cable News Network, 8 Mar. 2017, edition.cnn.com/2017/03/08/politics/fisa-court-explainer-trnd/index.html. Accessed 6 Sept. 2017.