ARTICLE 19
Free Word Centre,
60 Farringdon Road,
London, EC1R 3GA

Intelligence and Security Committee of Parliament
35 Great Smith Street,
London, SW1P 3BQ

Re: Response to the Privacy and Security Inquiry Call for Evidence

ARTICLE 19, international freedom of expression organisation, welcomes the opportunity to comment on the laws governing the intelligence agencies' access to private communications.

Before outlining our concerns, however, we must highlight that we are deeply concerned about the independence of the Committee in relation to the matter in hand. We believe the independence of the Committee is compromised on the grounds that:

- Secretaries of State can veto what information can be seen by the Committee;
- the Prime Minister's nomination is required for eligibility to sit on the Committee;
- the Prime Minister is responsible for determining which material the Committee can release publically.

We believe that this lack of independence reduces the Committee's ability to adequately command the confidence of the public on complex questions of whether the intelligence agencies have breached the law.

ARTICLE 19 is concerned about the following issues in the Call for Evidence.

- The Call includes misleading references to the "individual right to privacy" and the "collective right to security." We observe that both rights entail an individual and collective element. The right to security necessarily includes an individual right to security of the person. Equally, privacy entails a significant collective element – the right to privacy of collective gatherings such as societies, groups, and organisations as well as the crucial social function of privacy in encouraging free communication between members of society.

- The Call fails to acknowledge the extremely harmful impact of surveillance on the free flow of information and ideas. The UN General Assembly Resolution A/RES/68/167 on the right to privacy in the digital age, emphasises the vital importance of the right to privacy for the realisation of freedom of expression and its position as "one of the foundations of a democratic society." Furthermore, the resolution highlights that arbitrary surveillance, interception of communications and collection of personal data constitute a "highly intrusive" interference with both rights.

- The impact of surveillance on freedom of expression and access to information cannot be over stated. Just as people are much more likely to speak freely, if they know that their privacy is protected, the knowledge that their most private communications are highly likely to be inspected by others risks having a profoundly damaging effect on the free flow of information and ideas, to the detriment of all. It is also likely to deter whistleblowers from coming forward, individuals and groups from organising peaceful protests or expressing their views publically, and investigative journalism exposing corruption and wrongdoing – all activities vital to a strong democracy.

ARTICLE 19 also asserts that the current legal framework fails to ensure a strong protection of privacy and freedom of expression and puts journalists, civil society groups, and other actors at risk of arbitrary surveillance. To guarantee a healthy balance between and the right to freedom of expression, national security, and privacy, the laws governing surveillance should meet certain minimum criteria. It is vital for everyone that:

- communications data is given the same protection as the content of communications;
- access to data is authorised by a competent judicial authority; and
- there is effective public oversight of the implementation of surveillance laws and strong protection of whistleblowers.

For the reasons set out above, we enclose as an annex the *International Principles on the Application of Human Rights to Communications Surveillance*, signed by over 300 civil society organisations. The Principles provide a framework to evaluate whether proposed surveillance laws are consistent with a state's human rights obligations.

As the European Court of Human Rights recognised in *Klass v Germany* (*5029/71*), excessive surveillance laws "pose a danger of undermining or even destroying democracy on the ground of defending it." We strongly call upon the Intelligence and Security Committee of Parliament to ensure that any new proposals are in line with the Principles and protect our fundamental rights to freedom of expression and privacy. If the Committee does not make this call, Parliament risks undermining and threatening the very foundations of our democratic society.

Thomas Hughes
Executive Director
ARTICLE 19

ANNEX 1

International Principles on the Application of Human Rights to Communications Surveillance

1. As technologies that facilitate State surveillance of communications advance, States are failing to ensure that laws and regulations related to communications surveillance adhere to international human rights and adequately protect the rights to privacy and freedom of expression. This document attempts to explain how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques. These principles can provide civil society groups, industry, States and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights.

2. These principles are the outcome of a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology.

Preamble

3. Privacy is a fundamental human right, and is central to the maintenance of democratic societies. It is essential to human dignity and it reinforces other rights, such as freedom of expression and information, and freedom of association, and is recognised under international human rights law.[1] Activities that restrict the right to privacy, including communications surveillance, can only be justified when they are prescribed by law, they are necessary to achieve a legitimate aim, and are proportionate to the aim pursued.[2]

4. Before public adoption of the Internet, well-established legal principles and logistical burdens inherent in monitoring communications created limits to State communications surveillance. In recent decades, those logistical barriers to surveillance have decreased and the application of legal principles in new technological contexts has become unclear. The explosion of digital communications content and information about communications, or "communications metadata" - information about an individual's communications or use of electronic devices - the falling cost of storing and mining large sets of data, and the provision of personal content through third party service providers make State surveillance possible at an unprecedented scale.[3] Meanwhile, conceptualisations of existing human rights law have not kept up with the modern and changing communications surveillance capabilities of the State, the ability of the State to combine and organize information gained from different surveillance techniques, or the increased sensitivity of the information available to be accessed.

5. The frequency with which States are seeking access to both communications content and communications metadata is rising dramatically, without adequate scrutiny.[4] When accessed and analysed, communications metadata may create a profile of an individual's life, including medical conditions, political and religious viewpoints, associations, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications.[5] Despite the vast potential for intrusion into an individual's life and the chilling effect on political and other associations, legislative and policy instruments often afford communications metadata a lower level of protection and do not place sufficient restrictions on how they can be subsequently used by agencies, including how they are data-mined, shared, and retained.

6. In order for States to actually meet their international human rights obligations in relation to communications surveillance, they must comply with the principles set out below. These principles apply to surveillance conducted within a State or extraterritorially. The principles also apply regardless of the purpose for the surveillance -- law enforcement, national security or any other regulatory purpose. They also apply both to the State's obligation to respect and fulfil individuals' rights, and also to the obligation to protect individuals' rights from abuse by non-State actors, including corporate entities.[6] The private sector bears equal responsibility for respecting human rights, particularly given the key role it plays in designing, developing and disseminating technologies; enabling and providing communications; and - where required - cooperating with State surveillance activities. Nevertheless, the scope of the present Principles is limited to the obligations of the State.

Changing technology and definitions

7. "Communications surveillance" in the modern environment encompasses the monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects, arises from or is about a person's communications in the past, present or future. "Communications" include activities, interactions and transactions transmitted through electronic mediums, such as content of communications, the identity of the parties to the communications, location-tracking information including IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications.

8. Traditionally, the invasiveness of communications surveillance has been evaluated on the basis of artificial and formalistic categories. Existing legal frameworks distinguish between "content" or "non-content," "subscriber information" or "metadata," stored data or in transit data, data held in

the home or in the possession of a third party service provider.[7] However, these distinctions are no longer appropriate for measuring the degree of the intrusion that communications surveillance makes into individuals' private lives and associations. While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Today, each of these types of information might, taken alone or analysed collectively, reveal a person's identity, behaviour, associations, physical or medical conditions, race, color, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time,[8] or of all people in a given location, including around a public demonstration or other political event. As a result, all information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public, should be considered to be "protected information", and should accordingly be given the highest protection in law.

9. In evaluating the invasiveness of State communications surveillance, it is necessary to consider both the potential of the surveillance to reveal protected information, as well as the purpose for which the information is sought by the State. Communications surveillance that will likely lead to the revelation of protected information that may place a person at risk of investigation, discrimination or violation of human rights will constitute a serious infringement on an individual's right to privacy, and will also undermine the enjoyment of other fundamental rights, including the right to free expression, association, and political participation. This is because these rights require people to be able to communicate free from the chilling effect of government surveillance. A determination of both the character and potential uses of the information sought will thus be necessary in each specific case.

10. When adopting a new communications surveillance technique or expanding the scope of an existing technique, the State should ascertain whether the information likely to be procured falls within the ambit of "protected information" before seeking it, and should submit to the scrutiny of the judiciary or other democratic oversight mechanism. In considering whether information obtained through communications surveillance rises to the level of "protected information", the form as well as the scope and duration of the surveillance are relevant factors. Because pervasive or systematic monitoring has the capacity to reveal private information far in excess of its constituent parts, it can elevate surveillance of non-protected information to a level of invasiveness that demands strong protection.[9]

11. The determination of whether the State may conduct communications surveillance that interferes with protected information must be consistent with the following principles.

The Principles

12. **Legality:** Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit the right to privacy should be subject to periodic review by means of a participatory legislative or regulatory process.

13. **Legitimate Aim:** Laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner which discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

14. **Necessity:** Laws permitting communications surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim. Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification, in judicial as well as in legislative processes, is on the State.

15. **Adequacy:** Any instance of communications surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified.

16. **Proportionality:** Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy.

17. Specifically, this requires that, if a State seeks access to or use of protected information obtained through communications surveillance in the context of a criminal investigation, it must establish to the competent, independent, and impartial judicial authority that:

1. there is a high degree of probability that a serious crime has been or will be committed;
2. evidence of such a crime would be obtained by accessing the protected information sought;
3. other available less invasive investigative techniques have been exhausted;
4. information accessed will be confined to that reasonably relevant to the crime alleged and any excess information collected will be promptly destroyed or returned; and
5. information is accessed only by the specified authority and used for the purpose for which authorisation was given.

18. If the State seeks access to protected information through communication surveillance for a purpose that will not place a person at risk of criminal prosecution, investigation, discrimination or infringement of human rights, the State must establish to an independent, impartial, and competent authority:

1. other available less invasive investigative techniques have been considered;
2. information accessed will be confined to what is reasonably relevant and any excess information collected will be promptly destroyed or returned to the impacted individual; and
3. information is accessed only by the specified authority and used for the purpose for which was authorisation was given.

19. **Competent Judicial Authority:** Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

1. separate from the authorities conducting communications surveillance;
2. conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights; and
3. have adequate resources in exercising the functions assigned to them.

20. **Due process:** Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law,[10] except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of

flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.

21. **User notification:** Individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstances:

1. Notification would seriously jeopardize the purpose for which the surveillance is authorised, or there is an imminent risk of danger to human life; or
2. Authorisation to delay notification is granted by the competent judicial authority at the time that authorisation for surveillance is granted; and
3. The individual affected is notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time the communications surveillance has been completed. The obligation to give notice rests with the State, but in the event the State fails to give notice, communications service providers shall be free to notify individuals of the communications surveillance, voluntarily or upon request.

22. **Transparency:** States should be transparent about the use and scope of communications surveillance techniques and powers. They should publish, at a minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation type and purpose. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.

23. **Public oversight:** States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance.[11] Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to

communications surveillance. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

24. **Integrity of communications and systems:** In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes. *A priori* data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users as a precondition for service provision.[12]

25. **Safeguards for international cooperation:** In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from a foreign service provider. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

26. **Safeguards against illegitimate access:** States should enact legislation criminalising illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistle blowers, and avenues for redress by affected individuals. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through communications surveillance has been used for the purpose for which information was given, the material must be destroyed or returned to the individual.

References:

[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=35586

[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.

ENDS

ANNEX 2

Signatories to the International Principles on the Application of Human Rights to Communications Surveillance

Organisations

#YoSoyRed (México)

7iber (Jordan)

Access (International)

Acción EsLaRed (Venezuela)

ACTANTES (Brasil)

ActiveWatch - - Media Monitoring Agency (Romania)

Adil Soz - International Foundation for Protection of Freedom of Speech (Kazakhstan)

Africa Platform for Social Protection - APSP (Africa)

AGEIA Densi (Argentina)

AGEIA DENSI Colombia (Colombia)

Agenda Social y Política para las y los Jóvenes 2011-2021.México. (México)

Agentura.ru (Russia)

Agorà Digitale (Italy)

AgoraVox (France)

Aktion Freiheit statt Angst (Germany)

Aktionsforum Gesundheitsinformation (afgis) e.V. (Germany)

ALCONSUMIDOR A.C. (Mexico)

Alfa-Redi (Latin America and Caribbean)

All India Peoples Science Network (India)

Alternatif Bilişim Derneği (Alternatif Bilişim) - Turkey (Turkey)

Alternative Law Forum (India)

Amnesty International USA (USA)

April (France)

Arab Digital Expression Foundation (Egypt)

Arte Fora do Museu (Brasil)

ARTICLE 19 (International)

Articultores (Argentina)

ASL19 (Iran)

Asociación aLabs (Spain)

Asociación Civil por la Igualdad y la Justicia - ACIJ (Argentina)

Asociación Colombiana de Usuarios de Internet (Colombia)

Asociación de Abogados de Buenos Aires (Argentina)

Asociación de Internautas Spain (Spain)

Asociación para una Ciudadanía Participativa - ACI-Participa (Honduras)

Asociación Paraguaya De Derecho Informático Y Tecnológico - APADIT (Paraguay)

Asociación por los Derechos Civiles - ADC (Argentina)

Aspiration (United States)

Associação Brasileira de Centros de inclusão Digital – ABCID (Brasil)

Associação Coolpolitics (Portugal)

Associació Pangea Coordinadora Comunicació per a la Cooperació (Spain)

Association for Freedom of Thought and Expression – AFTE (Egypt)

Association for Progressive Communications - APC (International)

Association for Proper Internet Governance (Switzerland)

Association for Technology and Internet - APTI (Romania)

Association of Caribbean Media Workers - ACM (Trinidad and Tobago)

Association of Community Internet Center – APWKomitel (Indonesia)

Australia Privacy Foundation - APF (Australia)

Bahrain Center for Human Rights (Bahrain)

Bangladesh NGOs Network for Radio and Communication – BNNRC (Bangladesh)

BC Freedom of Information & Privacy Association (BC FIPA) (Canada)

Benetech (International)

Berlin Forum on Global Politics - BFoGP (Germany)

Big Brother Watch (United Kingdom)

Bits of Freedom (Netherlands)

BitValley Asociación Tecnológica (Spain)

Bolo Bhi (Pakistan)

Brasilian Institute for Consumer Defense - IDEC (Brasil)

British Columbia Civil Liberties Association - BCCLA (Canada)

British Columbia Library Association (Canada)

Bytes for All (Pakistan)

Cairo Institute for Human Rights Studies (Egypt)

Campaign for Press and Broadcasting Freedom (United Kingdom)

Canadian Association of University Teachers (Association Canadienne des Professeures et Professeurs D'université) (Canada)

Canadian Friends Service Committee (Canada)

Casa de Derechos de Quilmes (Argentina)

Center for Bangladesh Studies (Bangladesh)

Center for Democracy & Technology - CDT (United States)

Center for Digital Democracy (United States)

Center for Internet & Society India (India)

Center for Media Freedom & Responsibility - CMF (Philippines)

Center for Media Research - Nepal (Nepal)

Center for Media Studies and Peacebuilding (Liberia)

Center of Media Justice (United States)

Centre d'Etaudes Sur Les Conflitas, la Liberté, la Sécurité (CCLS) (France)

Centre for Community Informatics Research, Development and Training (Canada)

Centre for Law and Policy Research India (India)

Centre for Technology and Society - Scotland (Scotland)

Centro de Estudios en Libertad de Expresión y Acceso a la Información - CELE (Argentina)

Centro de formação profissional Alzira de Aleluia (Brasil)

Centro de Tecnologia e Sociedade (CTS) da FGV (Brasil)

Centrum Cyfrowe Projekt: Polska (Poland)

CESAR - Recife Center for Advanced Studies and Systems (Brazil)

Chaos Computer Club (Germany)

Chaos Computer Club Switzerland (Switzerland)

Chicago Alliance Against Racist and Political Repression (United States of America)

Chinese Association for Human Rights (Taiwan)

Citizen Lab (Canada)

Citizens Network Watchdog Poland (Poland)

Civil Initiative on Internet Policy (Kyrgyzstan)

Civil Rights Defenders (Sweden / Europe)

Civil Rights Society Vrijbit (Netherlands)

Civil Society Information Society Advisory Council - CSISAC (International)

Clínica de Nuevas Tecnologías, Propiedad Intelectual y Sociedad de la Escuela (Puerto Rico)

ClubComputer.at (Austria)

Coalition Against Gun Violence, a Santa Barbara County Coalition (United States)

Colaborativo México (México)

Collaboration on International ICT Policy in total East and South Africa - CIPESA (Uganda / East and Southern Africa)

Colnodo (Colombia)

Comisión Colombiana de Juristas (Colombia)

Comité Cerezo México (México)

Comité Cerezo México (Mexico)

Compliance Campaign (Denmark)

Computer Professionals' Union in the Philippines - CPU (Philippines)

Consumer Korea (South Korea)

Consumers International (International)

ContingenteMx (Mexico)

Cooperativa Autogestionaria Sulá Batsú R.L. (Costa Rica)

CORPECE (Ecuador)

Council for Civil Liberties - NSW CCL (Australia)

Cyber Arabs (Middle East)

CyberLaw Centre (Indonesia)

Datapanik.org (Belgium)

datapanik.org (Belgium)

DAWN Network (International)

Defending Dissent Foundation (United States)

DeJusticia (Colombia)

Delhi Science Forum (India)

Demand Progress (Rhode Island)

Deutsche AIDS-Hilfe e.V. (Germany)

Deutsche Vereinigung fuer Datenschutz e.V. (Germany)

Digital Courage (Germany)

Digital Enlightenment Forum (Belgium)

Digital Mayhem Radio (Canada)

Digital Rights Foundation (Pakistan)

Digitale Gesellschaft (Germany)

Digitale Gesellschaft Schweiz (Switzerland)

Digitterra (International)

DiploFoundation (Malta)

e-belarus.ORG (Belarus)

E-demokracija.si (Slovenia)

East European Development Institute (Ukraine)

Egyptian Initiative for Personal Rights (Egypt)

Electronic Frontier Finland - EFFI (Finland)

Electronic Frontier Foundation - EFF (International)

Electronic Frontiers Australia - EFA (Australia)

Electronic Frontiers Italy - ALCEI (Italy)

Electronic Privacy Information Center - EPIC (United States)

Environmental Protection Information Center - EPIC (United States / Northern California)

Espacio Público (Venezuela)

EthicsandGenetics (United Kingdom)

European Digital Rights - EDRI (Europe)

European Information Society Institute - EISi (Slovakia)

FACIL, pour l'appropriation collective de l'informatique libre (Québec, Canada)

Fantsuam Foundation (Nigeria)

Fight for the Future (United States)

Flüchtlingshilfe Iran e.V. 2010 (Germany, Berlin)

Förderverein freie Netzwerke e.V. (Germany)

Foro Ciudadano de Participación por la Justicia y los Derechos Humanos - FOCO (Argentina)

Foro de Periodismo Argentino - FOPEA (Argentina)

Forum InformatikerInne für Frieden und gesellschaftliche Verantwortung e. V. - FIfF (Germany)

Foundation No2-ID-nl (Netherlands)

Foundation No2-ID-nl (Netherlands)

Foundation for Community Educational Media - FCEM (Thailand)

Foundation for Information Policy Research – FIPR (United Kingdom)

Foundation for Media Alternatives - FMA (Philippines / Asia Pacific)

Free Network Foundation (United States)

Free Press (United States)

Free Press Unlimited (Netherlands)

Free Software Foundation Europe (Europe)

Free Software Movement of India (India)

Freedom Against Censorship Thailand (FACT) (Thailand)

Freedom of the Press Foundation (United States)

Freifunk (Germany)

Fundación AccesArte (El Salvador)

Fundación Ambio (Costa Rica)

Fundación Andina para la Observación y el Estudio de Medios (Ecuador)

Fundacion Comunica (Latin America)

Fundación Karisma (Colombia)

Fundación para la Libertad de Prensa - FLIP (Colombia)

Fundación Redes y Desarrollo - FUNREDES (Dominican Republic)

Fundación Sidar - Acceso Universal (Latin America)

Fundación Vía Libre (Argentina)

German Working Group on Data Retention (Germany)

Global Partners & Associates (United Kingdom)

Global Voices Advocacy (International)

Global Voices Advocacy in Spanish (Latin America)

GreenNet (United Kingdom)

Grupo de Software Libre de Cúcuta (Colombia)

Guerrilla Translation (Spain)

Gulf Center for Human Rights (Arab Gulf region)

Hackerspace Rancho Electrónico (Mexico)

Helsinki Foundation for Human Rights, Warsaw - HFHR (Poland)

Hermes Center for Transparency and Digital Human Rights (Italy)

Hiperderecho (Peru)

Hong Kong In-Media (Hong Kong)

Hong Kong In-Media (Hong Kong)

Hong Kong Journalists Association (Hong Kong SAR)

Human Rights Data Analysis Group (International)

Human Rights Watch - HRW (International)

HURIDOCS (Switzerland)

ICT Consumers Association of Kenya - ICAK (Kenya)

ICTWatch - Indonesian ICT Partnership (Indonesia)

Independent Journalism Center from Moldova (Republic of Moldova)

Index on Censorship (United Kingdom)

Information Technology Law (Belarus)

Initiative for Freedom of Expression (Turkey)

Initiative für Netzfreiheit (Austria)

Institute des Technologies de l'Information et de la Communication Pour le Developpement - INTIC4DEV (Togo)

Institute for Reporters' Freedom and Safety (Azerbaijan)

Institute for War and Peace Reporting - IWPR (United Kingdom)

Instituto Baiano de Direito Processual Penal - IBADPP (Brasil)

Instituto Bem Estar Brasil (Brasil)

Instituto Brasileiro de Direito Da Informática (Brasil)

Instituto Centroamericano de Estudios para la Democracia Social - DEMOS (Guatemala)

Instituto de Tecnologia e Sociedade - ITS (Brasil)

Instituto NUPEF (Brasil)

International Civil Liberties Monitoring Group (Canada)

International Commission of Jurist - Kenya Section (Kenya)

International Media Support - IMS (International)

International Modern Media Institute (Iceland)

Internet Governance Project, Syracuse University School of Information Studies (United States)

Internet Protection Lab (Netherlands)

Internet Society Belgrade Chapter (Serbia)

Internet Society Canada Chapter (Canada)

Internet Society German Chapter e.V. (ISOC.DE e.V.) (Germany)

Internet Society Palestine (Palestine)

Internet Society Poland (Poland)

Internet Society Trinidad and Tobago Chapter (Trinidad and Tobago)

InternetNZ (New Zealand)

Internews (United States)

Interzone Inc (International)

IP Justice (United States)

Iraqi Network for Social Media (Iraq)

Iriarte & Asociados (Peru)

ISOC - Philippine Chapter (Philippines)

ISOC Board of Trustees (International)

ISOC Congo Chapter (Congo)

ISOC Ecuador (Ecuador)

IT for Change (India)

Iuridicum Remedium, o.s. (Czech Republic)

Jan Philipp Albrecht MEP (Germany)

Jonction (Mauritania, Senegal, Tanzania)

Jordan Open Source Association (Jordan)

Journaliste en danger - JED (Congo)

Juliagruppen (The Julia Group) (Sweden)

JUSTICE (United Kingdom)

Kenya Human Rights Commission - KHRC (Kenya)

Kenya ICT Action Network - KICTANet (Kenya)

Kenyan Ethical and Legal Issues Network (Kenya)

Korean Progressive Network - JINBONET (Korea)

La Quadrature du Net (France)

Labdoo México (Mexico)

Lakome.com (Morrocco)

Latin American Network of Surveillance, Technology and Society Studies – LAVITS (Latin America and Caribbean)

Legal Agenda (Lebanon)

Liberty (United Kingdom)

Liga Uruguaya de Defensa del Consumidor (Uruguay)

Liga voor Mensenrechten vzw (Belgium)

Ligue Des Droits et Libertés (Québec, Canada)

Massachusetts Pirate Party (USA / Massachusetts)

May First / People Link (International)

Media Action Grassroots Network - MAG-Net (United States)

Media Development Centre (Macedonia)

Media Reform Coalition (United Kingdom)

Media Rights Agenda - MRA (Lagos, Nigeria)

Media@McGill (Canada)

Metamorphosis Foundation (Macedonia)

MOGiS e.V. - A Voice for Victims (Germany)

Movimento Mega (Brasil)

Mozilla México (México)

National Coalition Against Censorship - NCAC (United States)

National Union of Somali Journalists (NUSOJ) (Somalia)

Nawaat (Tunisia)

Netzwerk Recherche e.V. (Germany)

New York Chapter of the Internet Society (United States)

Norwegian P.E.N (Norway)

Observatorio Latinoamericano Para la Libertad de Expresión - OLA (Latin America and Caribbean)

Oneworld: Platform for Southeast Europe – OWPSEE (Western Balkans)

Ontario Humanist Society (Ontario, Canada)

Open Internet Tools Project - Open ITP (United States)

Open Knowledge Foundation (United Kingdom)

Open Media and Information Companies Initiative – Open MIC (United States)

Open Net Korea (South Korea)

Open Rights Group (United Kingdom)

Openmedia.ca (Canada)

Pacific Freedom Forum (Pacific Region)

Pakistan Press Foundation - PPF (Pakistan)

Palestinian Center for Development & Media Freedoms - MADA (Palestine)

Panoptykon Foundation (Poland)

Paradigm Initiative Nigeria - PIN (Nigeria / Africa)

Partidul Pirat Romania (Romania)

Partito Pirata Italiano (Italy)

Partners for Democratic Change Serbia (Serbia)

PEN American Center (United States)

PEN Canada (Canada)

PEN International (International)

People Who (International)

People's Solidarity for Participatory Democracy - PSPD (South Korea)

Pirata España (Spain)

Pirate Party Belgium (Belgium)

Pirate Party Germany (Germany)

Pirate Party of Greece (Greece)

Pirate Party of Russia (Russia)

Press Emblem Campaign PEC (Switzerland)

Privacy & Access Council of Canada (Canada)

Privacy Activism (United States)

Privacy First Foundation (Netherlands)

Privacy International (International)

Progressive Librarians Guild (USA / North America)

Projecto MiudosSegurosNa.Net (Portugal)

Protege QV (Cameroon)

Public Association "Journalists" (Kyrgyzstan)

Renewable Freedom Foundation (Germany)

Reporters Without Borders - RSF (International)

Réseau Koumbit (Canada / QC)

Russian Pirate Youth Project (Russia)

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic - CIPPIC (Canada)

Seattle Privacy Coalition (United States)

Serbian Library Association (Serbia, Belgrade 11000)

SHARE Conference | SHARE Defense (The Balkans)

Social Media Exchange (Lebanon)

SocialTIC (México / LATAM)

Society for Knowledge Commons (India)

Software Freedom Law Centre (India)

Software Liberty Association of Taiwan (Taiwan)

SonTusDatos.org (Mexico)

South East European Network for Professionalization of Media - SEENPM (South East Europe)

Southeast Asian Press Alliance (South East Asia)

Statewatch (United Kingdom)

Sulá Batsú (Costa Rica)

Support for Information Technology Center - SITC (Egypt)

Surveillance Studies Centre (Canada)

Surveillance Studies Network (International)

Swathanthra Malayalam Computing (India)

TagMeNot

Taiwan Association for Human Rights (Taiwan)

Tech To The People (Estonia)

TechLiberty (New Zealand)

Tecnologías Libres para Innovación y Desarrollo A.C. (Mexico)

TEDIC (Paraguay)

Telecápita (México)

Thai Netizen Network (Thailand)

The Communisphere Project (United States)

The International Federation of Library Associations and Institutions - IFLA (International)

The International Organization for the Security of Electronic Transactions – OISTE (Switzerland)

The KUKU Trust (Tanzania)

The Library Association of the Republic of Kazakhstan (Kazakhstan)

The Mother and Child Health and Education Trust (Hong Kong)

The New Renaissance Network (Sweden)

The Open Source Shoppe (India)

The Pacific Islands News Association - PINA (Pacific Islands)

ThoughtWorks (International)

TMPLAB (France)

TransMediar-Pimentalab [at] Universidade Federal de São Paulo (Brasil)

Uganda Harm Reduction Network(UHRN) (Uganda)

Ultimate Circle (Belgium)

University of Campinas - Research Group CTeMe (Knowledge, Technology and Market) (Brasil)

University of São Paulo's Research Group on Access to Information Policies (GPoPAI-USP) (Brasil)

Unwanted Witness (Uganda)

Ushahidi (International)

VECAM (France)

VIBE!AT (Austria)

Voices for Interactive Choice and Empowerment (Bangladesh)

West African Journalists Association (Mali)

Wikimedia México (México)

WITNESS (International)

Wlan Slovenija (Slovenia)

World Association for Christian Communication - WACC (Global)

Zimbabwe Human Rights NGO Forum (Zimbawe)

Zwiebelfreunde e.V. (Germany)

Experts, Academics & Prominent Individuals

Andrew A. Adams, Professor of Information Ethics at Meiji University in Tokyo (Japan)

Rasha A. Abdulla, Ph.D. Associate Professor. Former Chair Journalism and Mass Communication The American University in Cairo (Egypt)

Ali Hasan Abunimah, Palestinian-American journalist who has been described as "the leading American proponent of a one-state solution to the Israeli-Palestinian conflict. (United States)

Alessandro Acquisti, Associate Professor of Information Technology and Public Policy, Heinz College, Carnegie Mellon University, Co-Director, CMU Center for Behavioral Decision Research (United States)

Hisham Almiraat, Advocacy Director, Global Voices Advocacy (Morocco)

Axel Arnbak, Fellow Berkman Center, Harvard University and Center for Information Technology Policy Princeton. Researcher at Institute for Information Law, University of Amsterdam. (Netherlands)

Dr. Reza Aslan, an internationally acclaimed writer and scholar of religions, is author of the #1 New York Times Bestseller Zealot: The Life and Times of Jesus of Nazareth. (Iran)

Sami Ben Gharbia | بن سامي Founding Director of Global Voices Advocacy Co-founder of the Tunisian award-winning collective blog nawaat.org (Tunisia)

Benjamin G. Davis, Associate Professor of Law, University of Toledo College of Law (United States)

Yochai Benkler, Jack N. and Lillian R. Berkman Professor for Entrepreneurial Legal Studies, Faculty Co-Director, Berkman Center for Internet and Society (United States)

Colin J. Bennett, Department of Political Science, University of Victoria (Canada)

Paul Alexander Bernal, Lecturer in IT, IP and Media Law UEA Law School, University of East Anglia Norwich Research Park (United Kingdom)

Caspar Bowden, privacy advocate, formerly chief privacy adviser at Microsoft. (United Kingdom)

Danah Boyd, Principal Researcher, Microsoft Research and Research Assistant Professor, New York University (United States)

Dr. Ian Brown, Associate Director of Oxford University's Cyber Security Centre, and Senior Research Fellow at the Oxford Internet Institute (United Kingdom)

Beatriz Busaniche, Professor, Social Sciences, University of Buenos Aires (Argentina)

Yang Cao, Vice Director of Intellectual Property Research Center, Associate Professor of Law, Shanghai University of Political Science and Law (China)

Andrew Clement, Professor, Faculty of Information, University of Toronto (Canada)

Ray Corrigan, Senior Lecturer in Maths, Computing and Technology, Open University (United Kingdom)

Simon Davies, Founder Privacy International. Editor The Privacy Surgeon (United Kingdom)

Cory Doctorow (United Kingdom)

William J. Drake, International Fellow & Lecturer Media Change & Innovation Division, IPMZ University of Zurich, Switzerland (United States)

Julie E. Cohen, Professor of Law at the Georgetown University Law Center. (United States)

Michael Froomkin, Laurie Silvers and Mitchell Rubenstein Distinguished Professor of Law, received an M.Phil. degree from Cambridge University in 1984, and a J.D. from Yale Law School in 1987. (United States)

Gemma Galdon Clavell, Polítiques i tecnologies de seguretat / Security, Technology & Society, Universitat de Barcelona (Spain)

Michael Geist, Canada Research Chair in Internet and E-commerce Law, University of Ottawa (Canada)

Dan Gillmor, Director of the Knight Center for Digital Media Entrepreneurship, Arizona State University's Walter Cronkite School of Journalism and Mass Communication (United States)

David H. Flaherty, Ph.D., Professor Emeritus of History and Law, University of Western Ontario. Former Information and Privacy Commissioner for British Columbia (Canada)

Wafa Ben Hassine, Writer and Human Rights Advocate (Tunisia)

Christian Horchert, IT-Security Consultant, Member of Chaos Computer Club and Digitale Gesellschaft (Germany)

Rey Junco, Associate Professor of Library Science at Purdue University (United States)

Rikke Frank Jørgensen, Special Adviser, PhD., Research, The Danish Institute for Human Rights (Denmark)

Douwe Korff, Professor of International Law, London Metropolitan University since 2002. (Netherlands)

Dr Maria Kutar, Senior Lecturer in Information Systems, Salford Business School, University of Salford (United Kingdom)

Rebecca Mackinnon, Co-Founder, Global Voices Online and Author, "Consent of the Networked." (United States)

Morgan Marquis-Boire, Security and Human Rights Researcher (New Zealand)

Pablo A. Palazzi, Profesor de Derecho Universidad de San Andrés (Argentina)

Christopher Parsons, Postdoctoral Fellow at the Citizen Lab in the Munk School of Global Affairs, University of Toronto (Canada)

Jon Penney, Research Fellow at the Citizen Lab, Munk School of Global Affairs, University of Toronto. (Canada)

Professor Charles Raab, Professor of Government, School of Social and Political Science, University of Edinburgh (United Kingdom)

Siva Rama Krishna T, Assistant Professor of Computer Science, University College of Engineering Vizianagaram, Jawaharlal Nehru Technological University Kakinada (India)

Neil M. Richards, Professor of Law Washington University, St. Louis (United States)

Nagla Rizk, Professor of Economics; Founding Director, Access to Knowledge for Development Center (A2K4D); School of Business, The American University in Cairo; Faculty Associate, Berkman Center for Internet and Society (Egypt)

Patrick Ryan, Senior Affiliated Researcher, Katholieke Universiteit Leuven (Belgium)

Bruce Schneier, internationally renowned security technologist (United States)

José María Serralde Ruiz, pianista, artista multidisciplinario, y activista del software y la cultura libre. (Mexico)

Professor Peter Sommer, expert in criminal and civil court proceedings where digital evidence has been an issue. Visiting Professor, De Montfort University Cyber Security Centre. (United Kingdom)

Jennifer Stisa Granick, Director of Civil Liberties Stanford Center for Internet and Society (United States)

Siva Vaidhyanathan, Chair Department of Media Studies Robertson Professor University of Virginia Department of Media Studies & School of Law (United States)

Nigel Waters Pacific Privacy Consulting (Australia)

ENDS