International Working Group
on Data Protection
in Telecommunications

675.50.14

Working paper on Transparency Reporting:

Promoting accountability when governments access personal data held by companies

57th meeting, Seoul, 27-28 April 2015

"Doveryai, no proveryai."
- Russian proverb quoted by Ronald Reagan meaning "trust, but verify"

"When every detail is given, the mind rests satisfied, and the imagination loses the desire to use its own wings."
- Thomas Bailey Aldrich, American poet and writer

"The secretive nature of security surveillance in many places inhibits the ability of legislatures, judicial bodies and the public to scrutinize State powers. This lack of transparency … creates serious obstacles to ensuring that these powers are not used in an arbitrary or indiscriminate manner."
- Navi Pillay, United Nations High Commissioner for Human Rights

Scope

This paper explores the usefulness for data protection and privacy purposes of transparency reporting by telecommunications companies and online services providers. Transparency reporting is useful for promoting trust in organisations with substantial holdings of personal data and contributes to holding public authorities accountable for their practices in seeking access to such data.

'Transparency reporting' is used in this paper to mean the periodic public reporting by data controllers or data processors of statistics, and supporting explanations, of details of personal information released to third parties for non-business purposes. The paper principally focuses upon releases to law enforcement[1] and national security organisations without precluding other types of non-business releases.[2]

Although the paper's principal focus is upon reporting by private sector organisations involved with telecommunications, the paper's observations and recommendations may also usefully be relevant to public bodies and to organisations operating outside the telecommunications sector.[3]

[1] 'Law enforcement organisations' for the purposes of this paper is understood to include regulatory bodies as well as criminal law enforcement bodies. In many jurisdictions regulatory bodies, government departments and local government bodies frequently seek access to company information.
[2] Examples of other releases would be those following upon emergencies or security breaches.
[3] For example, the financial services sector or the credit reporting industry.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The paper does not directly cover the related topics of the justification for law enforcement or national security access to organisations' records or data, the proper lawful limits on such access, or the authorisation and control of intrusive surveillance practices by investigative bodies.[4] A number of other working group papers touch on these topics and may usefully be read in conjunction with this paper.[5]

The working group supports the practice of transparency reporting given its potential to promote accountability in the processing of personal data. Organisations undertaking transparency reporting should ensure that the reported statistics are reliable, informative and internationally comparable.[6]

Background

Governments properly need on occasion to obtain access to records held by private bodies in order to perform public functions.[7] A traditional example is an audit of a company's records to verify that the correct tax has been paid. For decades, governmental demands for privately-held records have gradually been increasing giving rise to civil liberties and business compliance cost concerns. Governmental demands for access to company information, and particular information held about individuals, has grown in scope and volume substantially since 2001. This growth reflects a growing attractiveness to governments of private sector data arising from a convergence of multiple technological and business factors including:

- *Data availability:* Data storage costs have substantially dropped – and continue to drop - making long term storage of large volumes of transactional data feasible.
- *Processing power:* There have been major advances in the ability to quickly correlate, process and analyse huge holdings of data. Big data has become big business.[8][9]
- *Specialised techniques now mainstream:* Once the preserve of the few, many specialised data-based analytical practices have become standard in business (and government) such as predictive analysis, contact chaining, data visualisation and network analysis.

---

[4] For a discussion of many of the broader privacy policy issues in this context see Centre for Democracy and Technology, *Systematic Access to Government Data: A Comparative Analysis*, 2013. Earlier case studies on Systematic Government Access to Private-Sector Data available at http://idpl.oxfordjournals.org/content/2/4.toc.

[5] All IWGDPT working papers are available at http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group. For example, see IWGDPT Working Paper on the Human Right to Telecommunications Secrecy (Berlin, September 2013) and The Granada Charter of Privacy in a Digital World (Granada, April 2010).

[6] While transparency reporting by companies is often undertaken voluntarily, there may be some jurisdictions that prescribe more specific reporting requirements and report formats. Such requirements naturally prevail over the general guidance in this paper. While international comparability to the extent possible remains desirable, additional locally-imposed requirements can still be valuable in promoting more fine-grained comparability within sectors and individual jurisdictions.

[7] For convenience, this paper refers to these as 'company' information or records. This is to emphasise that the focus is principally upon government requests made to private sector data controllers or data processors.

[8] See IWGDPT Working Papers on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics (Skopje, May 2014) and on Cloud Computing – Privacy and data protection issues (Sopot, April 2012).

[9] See 36th International Conference of Data Protection and Privacy Commissioners (ICDPPC), Resolution on Big Data, Mauritius 2014, and 34th ICDPPC, Resolution on Cloud Computing, Uruguay 2012. ICDPPC resolutions are available at www.icdppc.org.

- *New business models:* Novel and profitable businesses have emerged that are built upon the analysis of transactional data and the interconnection of datasets. Cloud services providers hold information from many companies outside any individual company's systems.
- *Shift from oral to written message forms:* The transition from analogue to digital telephony enabled convenient data services such as SMS that encouraged consumers to replace impermanent oral communications with written messages susceptible to longer term storage. Mass adoption of mobile telephony and smart phones has hastened the trend.
- *Massive personal data traces created unperceived by individuals:* The move from analogue to digital telephony has generated more traffic data that is susceptible to storage and analysis. Smart mobile telephony and GPS has enabled geolocation services that create sensitive information traces that never previously existed. Added to this are a growing universe of sensors and the construction of the 'Internet of Things' which will generate data associated with individuals, often without any human intervention.
- *User-generated content:* Internet services and, more recently, social media, have changed consumer behaviours so that many people now record and publish their own personal and transactional details in such a way that governments can easily access them through company records or even by bypassing company controls altogether.[10]

However, those technological and business factors alone cannot explain the growth in government access. Additional factors on the government side of the equation include:

- *Public-private linkages:* Public-private sector boundaries have blurred. Private sector practices have been replicated in the public sector. Former public utilities, with access to core data on entire communities, have been privatised with the services performed, and data held, in the private sector. Governments have become a player in the private sector data eco-system both as a source of data and as a consumer of data services. Private companies have become major players in investigation and security work.
- *Law enforcement and national security:* Since 2001, there has been a greater willingness by the public, legislatures and courts to allow national security and law enforcement concerns to prevail over traditional norms of company confidentiality. Law enforcement concerns have manifested themselves in many areas with two well-known ones being aviation[11] and financial services.[12] Traditional governmental access to company data based upon targeted investigation of individuals suspected of wrong-doing has been supplemented by general surveillance of entire populations by means of analysis of huge data sets to detect activities or persons of interest. Thresholds for authorising surveillance have been lowered in many jurisdictions together with a broadening of the amount of information that might be gathered under a single warrant. Transactional data is now more routinely monitored in mass systems of surveillance in many countries rather than solely on the basis of an individualised investigation.
- *Rewiring telecommunications systems to suit governmental interests:* Traditionally governments have been content to seek access to company records when those records existed and where applicable company systems made access feasible. However, governments have in recent years recalibrated the relationship between public and private sector and many have enacted laws, and come to arrangements with network providers, to require the creation at substantial

[10] This paper concerns only those cases in which records are sourced through companies. Any privacy and accountability issues associated with government accessing of information that is publicly available, or by bypassing company controls, are not covered here.

[11] There has been a particular focus on transactional information on travellers (often referred to as 'Passenger Name Record' or PNR information). See 29th ICDPPC, Resolution concerning the safeguarding of passenger data, 2007.

[12] The emphasis has particularly been on money laundering and the financing of terrorism.

cost of 'back doors' to enable governmental access into systems where such access would not have been necessary for business purposes.[1314]

- *Shifting the burden from government to companies*: The use of traditional search warrants, while remaining a vital part of criminal investigations, imposed a substantial administrative burden on the state and new legal tools have been developed which shift the burden of locating, assembling and producing documentation for government inspection onto companies.[15]
- *Reordering data storage requirements to meet governmental interests*: Governments have not merely required companies to assemble and produce documentation that they hold for government inspection but have required companies to retain documentation for extended periods – beyond any actual business need - in case the government might need to access the information in the course of an investigation.[16]

Collectively, such factors have come together to make information held in the private sector an even more attractive source of information for governments than had previously been the case. Huge repositories of information have become available for governments where previously information would have been absent or inaccessible. The information is often now held conveniently, from a governmental point of view, by information service providers and on networks rather than isolated within individual companies. Information of interest is often interconnected with additional information multiplying its value. Traditionally, the vastness of the data available would have been an insurmountable barrier to useful or timely analysis. However, the growth in computing power and advances in processing techniques allow governments to be fairly ambitious in their data harvesting and analytical projects. The changes have meant that information is now available for governments either to collect in bulk or access at will.

The environment in which such projects are initiated has become more conducive to government interests. A series of high profile terrorism incidents has resulted in a level of public anxiety and provided the justification for national security and law enforcement projects to extend the hand of government ever further into company records.

Numerous laws have been enacted since 2001 granting law enforcement authorities greater access to company information. Traditionally, these laws would precisely state the limits of access and set out the lawful processes by which powers could be exercised. Typically, in the past a judicial warrant might have been required to access company records. However, in the electronic environment new paradigms may be emerging in relation to state powers. While legislatures have often sought to

---

[13] Many countries require that digital telephony systems providing services to the public be rendered capable of interception – a clear example of governmental interests having priority over privacy of communications. A number of countries also ban anonymous cell phone accounts.

[14] Arguably, state demands to create 'back door' are not entirely novel and have existed previously with some postal, telegraph and analogue systems. Such access was especially easy for governments in earlier years where the state may have owned the telecommunications systems or could deal with a single monopoly provider. However, the trend still seems noteworthy as the state has not merely required administrative access to systems but substantial and costly systems changes that may affect many companies and sometimes run counter to legitimate company desires to create secure networks.

[15] These powers are sometimes referred to as 'production orders' or 'assistance orders'.

[16] For example, in the telecommunications sector, many countries impose retention requirements for storage of call traffic records beyond their need for business purposes. In the banking sector, most countries require long term storage of copies of customer account identification documents as part of anti-money laundering 'know your customer' requirements while in the telecommunications sector some countries outlaw anonymous cell telephone accounts and require retention of customer account identification documents.

maintain traditional norms, the constant expansion of laws and calls for 'future proofing' have created more elastic concepts and these have invariably expanded access.[17]

While the extent of lawful authority of law enforcement authorities is occasionally unclear, this is almost always the case with intelligence and security organisations with a national security mandate. The limits on powers and safeguards on exercise of powers are usually less robust or transparent when national security objectives are cited than in law enforcement and the scope of information that might be accessed is understood usually to be much broader.

In addition, both law enforcement investigations and national security intelligence gathering are frequently undertaken in secret. However, once the investigative phase is complete, a degree of transparency is introduced into law enforcement proceedings given the role of open justice in a free society governed by the rule of law. Law enforcement authorities will normally put allegations to the accused person and give them a chance to explain themselves. If the matter proceeds to a prosecution, the accused person's lawyer will be given relevant documentation and a public hearing in open court. Conversely, national security intelligence gathering is always shrouded in secrecy and since prosecution of individuals is not necessarily the intended or actual outcome, the veil of secrecy may never be lifted. The cases that are brought to public attention are likely to be a tiny proportion of the overall surveillance activity.

In a democratic society, activities undertaken by state authorities in secret are usually viewed with suspicion and create mistrust.[18] Attempts to promote public trust by establishing a degree of oversight over national security organisations have sometimes floundered when the state authorities have been shown to have misled the public and even the oversight bodies.[19]

Accordingly, while it can be confidently stated that governments are seeking and obtaining far more access to personal data contained in company hands than has formerly been the case, the precise extent of that access is somewhat unclear. It is within this context that transparency reporting may have a useful role to play.

Transparency reporting

For each instance of government access to company records or information for non-business purposes, there will be a government agency that seeks the information and a company that receives the request and acts upon it. This paper is principally focused on reporting the actions of the companies that receive such requests. Although not the focus of this paper, it should be emphasised that transparency and accountability of public bodies that request or require companies to release their records to the government is equally vital. The working group has previously emphasised the importance of transparency as an element of accountability for state interception of private communications or surveillance.[20]

---

[17] Examples include less stringent requirements to access meta-data and new processes to monitor dynamic data environments in real time. It is quite likely that while the authorities that seek more flexible language in law understand the ramifications, most lawmakers have a very limited understanding of what they are permitting.

[18] See Report of the European Parliament on the US NSA Surveillance Programme, surveillance bodies in various member states and their impact on EU citizens' fundamental rights an on trans-Atlantic cooperation in Justice and Home Affairs, February 2014

[19] For example, see the United States Senate Select Committee on Intelligence Study of the Central Intelligence Agency's Detention and Interrogation Program, released December 2014.

[20] IWGDPT Working Paper on Telecommunications Surveillance (Auckland, 2002) and IWGDPT Common Position on Public Accountability in relation to Interception of Private Communications (Hong Kong, 1998).

The growth in government demands for company records and personal data has been of concern not only to individuals and privacy advocates but also to the companies themselves. Some of the company concerns have been prosaic concerns over the compliance costs (which can be considerable). Other company concerns relate to the ethical difficulty of reconciling the release of confidential personal data to state authorities for non-business purposes with the relationship of trust they seek to maintain with their customers and other business partners.

There are also worries about legal liability when companies are subject to competing legal responsibilities to protect security and confidentiality and also comply with access requests from state authorities in a particular jurisdiction. The legal complexities multiply when the company is a multi-national operating in several jurisdictions and there is a conflict of laws or the request is made of a processor to covertly release another company's data. There are additional complexities in the context of cross-border requests under mutual assistance treaties.[21]

One solution that companies may adopt is to develop a clear and rigorous company policy for handling government requests to ensure that they are competently and legally handled and mistakes are avoided. Typically, policies may involve centralisation of requests, standardised handling, clear company criteria aligned with applicable legal requirements and involvement of senior and experienced staff. Internal audit, monitoring and reporting to senior management are usual requirements. Companies may require a search warrant or similar legal instrument before releasing records. Attention to good practice, ethical concerns and company reputation has led many companies to consider the place of public reporting.

Google published its first transparency report in 2009 followed by a handful of telecommunications and internet services companies in the next 3 years.[22] However, the practice really took off in 2013 with dozens of companies publishing transparency report in North America, Europe, Asia and Australasia.[23]

Companies do not typically explain in detail why they publish transparency reports although many state that privacy is important to their company. As it is not generally a legal obligation to release such reports, the motivation probably rests on reputational concerns and on the company's view of itself as a responsible corporate citizen. Behaviour of peers may sometimes be a factor. Publication of a report may be an attempt to show that a company remains worthy of any trust vested in it as it is demonstrating that it is doing its best professionally to perform the difficult dual roles of cooperating with lawful demands while maintaining responsibilities of security and confidentiality. Properly handling demands for access to records – and publicly reporting on its actions in that context – are both viewed as exercises in accountability to customers, business partners and the wider public.

In a sense, transparency reporting by companies is an attempt by private sector bodies to hold public bodies accountable. Public bodies ultimately are responsible for the access demands that create public unease or run counter to customer expectations but it is companies that are faced with releasing the information. Publishing reports that account for the actions they have been compelled to perform are an attempt to call on public bodies to account for their actions. There are practical reasons behind company attempts to hold public authorities to account and some benefits may result. Dealing with multiple demands for access comes at a compliance cost to a company. If that company meekly complies they may be marked out as a 'soft touch' by the authorities and become a favoured first port of call for information. Shining a light onto the practices by transparency reporting

[21] See, for example, Global Network Initiative, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, January 2015.

[22] At least 12 companies were publishing transparency reports on-line by 2012. Source: Office of the Privacy Commissioner, New Zealand.

[23] Some 37 on-line company transparency reports have been located for 2013. Source: Office of the Privacy Commissioner, New Zealand.

may help ensure that authorities take greater care to ensure that their use of their coercive powers is proportionate and justifiable. Companies might be said to be trying to restore the ethos of 'open government' which has suffered a setback in the area of government surveillance.

Release of company information to a third party for a non-business purpose, without consent from the individual concerned and probably contrary to the individuals' wishes and interests, is obviously challenging from a data protection perspective. However, this has always been the case for law enforcement cases and the dilemma has generally been resolved by recognising law enforcement investigations as a legitimate exception to non-disclosure expectations. However, the challenge in the current environment relates to the growth in access to company information as a routine rather than exceptional investigative technique and to the bulk release and real-time access to company information for surveillance purposes.

To respond to these challenges to traditional data protection expectations, greater attention is now being paid to the need for both public bodies and companies to demonstrate that they are accountable in their information handling practices. Transparency is seen as an important part of this. It might be seen as a social compact under which citizens expect their communications and affairs to be maintained in confidence subject only to lawful and proportionate law enforcement and national security exceptions with the relevant organisations subject to trustworthy independent oversight. Transparency reporting is one form of public 'auditability' to ensure that the terms of the compact are adhered to.

Reporting informs the public in a general way about the actions of public authorities. Public reporting by both the bodies making access demands and those acting on those demands promotes accountability of both sets of key players. The reports ultimately also inform the public and legislatures who ultimately decide where they wish the line to be drawn on surveillance and liberty.

Content of transparency reports

The ad hoc growth of voluntary company transparency reporting has resulted in multiple series of statistics that are not always comparable with each other.[24] The level of granularity varies, metrics differ and there is a diversity (or lack of) data definitions.

However, there is scope for bringing order into the system of reporting as the basic approach of most transparency reports is fairly similar. The reports give relevant statistics on the number and nature of government requests for company information and on the outcome of those requests. The reports may also conveniently capture other types of reporting relevant to the company in question – such as copyright take down requests or European 'right to be forgotten' requests to break web links – but as useful as those additional reports are they are outside the scope of this paper.

To briefly elaborate on the typical aspects of transparency reports:

- *Jurisdiction:* Companies operating in multiple jurisdictions are likely to receive requests from government authorities in different countries and the structure of the report will need to reflect that. Different countries will use different terminology for similar concepts and the company will need to decide whether to use standard terminology across all jurisdictional reports or to align the language to statutory terminology from a particular jurisdiction. One useful technique is to use standardised terminology but to provide a key, or footnotes, explaining how the terms are used in relation to each jurisdiction.

[24] The problems arising from lack of standardisation of reports are highlighted in Christopher Parsons, *Do Transparency Reports Matter for Public Policy? Evaluating the Effectiveness of Telecommunications Transparency Reports*, 2015, available at SSRN: http://ssrn.com/abstract=2546032 or http://dx.doi.org/10.2139/ssrn.2546032.

- *Reporting period:* Transparency reporting is not a one-off exercise but is a continuing process. While real time online reporting might be feasible in the future, the practice so far has been for companies to report annually with larger companies reporting more frequently at quarterly or half yearly intervals. Reports will usually track trends and may provide graphs and commentary that compares current figures with previous periods.
- *Request types:* Government requests come in different forms and most reports seek to standardise those in ways appropriate to the jurisdiction and industry. Typical classifications may relate to the legal form of the request (e.g., a judicial warrant or an administrative request), the nature of the action being asked of the company (e.g., to access existing records or to place a device that will continue to monitor an account and release activity data to the government in real time), whether the request arises under criminal or civil law and whether the request comes from a domestic or foreign law enforcement authority.[25] There are many sub-categorisations that may also usefully be made. Companies tend to structure their reports around the most numerous requests, usually those received in their home jurisdiction.
- *Number of requests:* The starting point for reporting must naturally be the requests received from government. Very simple reporting of the number of requests might conceal substantial differences in the nature and scale of requests. Accordingly, the more useful reports will capture both the number of requests received and the number of individual records or accounts to which those requests relate.
- *Volume of information or affected individuals:* Appearing in some, but not all reports, are figures characterising the scale and impact of the requests.
- *Outcome of requests:* Transparency reports do not simply reflect what the government has asked of companies. They also account for the company's actions and thus the outcome of the request. This might differ depending upon the nature of the company, the character of the requests and applicable law. For example, a data processor should refer any government request for access to the relevant data controller unless the law prohibits the processor from taking that step. A report for a data processor therefore might include statistics on the number of references to client data controllers and the number of cases where the processor directly answered the request. Generally, most reported statistics will relate to the acceptance or refusal of requests and, where access was given, there would be details of the number of records, individuals or accounts affected. In some cases, there will be legal controls limiting or delaying the publishing of statistics.
- *Commentary:* Statistics will typically be accompanied by an introduction, explanation of terms used and commentary on trends. Special comment may be offered on unexpected or exceptional figures.

Transparency Reporting Principles

The working group recommends that privacy and data protection authorities encourage companies to adopt the following 'principles' of transparency reporting:

1. ***Principle of accountability***: Companies should be accountable for their actions in handling government requests to release information for non-business purposes.

2. ***Principle of transparency***: Companies that are routinely subject to government requests to release information for non-business purposes should periodically report publicly on the nature and quantity of the releases.

3. ***Principle of reliability***: Company transparency reports accounting for the release of personal information in response to government requests should be accurate and complete.

[25] Companies might refuse to process requests from foreign authorities and record that in their reports.

4. ***Principle that reports should not mislead*:** Notwithstanding that laws may sometimes impose delays or limits on reporting,[26] companies that publish transparency reports should take steps to avoid any misleading impression through presentation of incomplete statistics.

5. ***Principle of comparability*:** Companies should seek to ensure that reported statistics may be meaningfully compared with previously published reports and with the statistics included in other transparency reports.

6. ***Principle of accessibility*:** Transparency reports should be published in a form and in a place in which they can most effectively be accessed by the public, the news media and relevant stakeholders.

Recommendations to give effect to principles

Transparency reporting has, so far, been a voluntary initiative driven from the private sector in response to governmental inroads on public expectations of privacy. The working group supports the initiative and recommends that transparency reporting should be enhanced and extended to more companies and sectors. The individual companies that have already commenced transparency reporting are to be congratulated. However, it is difficult for any individual company to achieve a goal such as the comparability of published statistics. Nor can any individual company achieve transparency throughout an entire sector. However, collectively the more companies that undertake this practice, the more complete a picture will emerge of governmental actions and the corresponding actions of companies that are the stewards of citizen's personal data. Once prominent companies have begun transparency reporting, market pressure may build on competitors to be more transparent.

The working group takes the view that in addition to individual companies, other stakeholders have a part to play to promote and enhance transparency reporting. Therefore these recommendations are addressed to both companies and other stakeholders and seek better to give effect to the transparency principles.

The working group recommends:

Companies

(a) Companies subject to government requests for access to personal information they hold should:
   i. Adopt reliable processes for the receipt and handling of requests from government for access to personal information to ensure that releases of information are handled in a manner that is accountable, legally compliant and consistent with the company's policies.
   ii. Publish their policies for the handling of government requests.
   iii. In the case of companies that repeatedly receive requests from governments for access to personal information they hold, adopt the practice of transparency reporting as discussed in this paper.
   iv. Ensure that transparency reports they publish are reliable by ensuring that statistics are soundly produced and verifiable.
   v. Structure their reports and terminology in ways that promote the comparability of statistics across companies, sectors, countries and time periods.

[26] It is to be understood in offering these principles that companies need to be compliant with applicable national law in undertaking transparency reporting.

vi. Avoid practices that might mislead readers and, in particular, if reported figures are incomplete by reason of government restrictions to note the incompleteness and to publish complete figures when the restrictions expire.
vii. Support efforts to more effectively disseminate reports by, for example, assisting efforts to republish figures in common national or international repositories.
viii. Track the consistency of their reporting practices with the transparency reporting principles and enhance as needed.

Government rule making

(b) Governments establishing laws or rules under which public authorities may seek access to personal information held by companies should:
   i. Ensure that laws and rules remain within reasonable limits that are proportional to the public interests involved, contain appropriate safeguards and provide means to hold public authorities accountable.
   ii. Ensure that there are obligations to promote transparency in the use of such powers.
   iii. Remove unnecessary legal barriers to transparency reporting.
   iv. Provide for mandatory statistical reporting by public authorities of the use of powers to access company information.

Public authorities seeking access to company information

(c) Public authorities should:
   i. Use powers to access company information in a lawful, proportionate and accountable manner.
   ii. Be transparent in their use of powers including, for example, through regular statistical reporting on the exercise of powers.
   iii. Avoid imposing secrecy requirements that are excessive to the reasonable needs of law enforcement or national security.
   iv. Review any existing secrecy requirements to ensure that they do not exceed what is justifiable in a free society.

Data Protection Authorities

(d) Data protection authorities should:
   i. Support the efforts of companies that have voluntarily adopted transparency reporting and encourage and support other companies to do so.
   ii. Promote better practice in transparency reporting to encourage the production of meaningful statistics that are reliable and comparable nationally and internationally.
   iii. Support or initiate efforts to make transparency reports more accessible on centralised national or international repositories.
   iv. Make use of the information revealed through the reports to inform their work.

International Governmental Organisations

(e) International organisations should:
   i. Encourage the development of internationally comparable metrics to inform the policy making process related to privacy and the transborder flows of personal data.
   ii. Identify areas where government secrecy requirements operate as an unnecessary barrier to transparency and promote better practices to governments that support openness and build online trust.

Telecommunications regulators

(f) Telecommunications regulators should:

i. Support and encourage the practice of transparency reporting in the telecommunications sector.

Industry groups

(g) Industry groups should:

i. Give guidance as to best practice transparency reporting relevant to their industry in consultation with relevant stakeholders such as data protection authorities and civil society.[27]

Civil Society

(h) Civil society should:

i. Demand accountability from all relevant entities (governments that establish laws permitting access, public authorities that seek access to company information, companies that handle government requests and release personal information for non-business purposes).
ii. Encourage companies to adopt transparency reporting.
iii. Support the establishment of common repositories to access reports.[28]
iv. Make use of statistics produced through transparency reporting.

[27] An example of such an industry initiative is the Telecommunications Industry Dialogue which bases its activities around the UN Guiding Principles on Business and Human Rights, including operational principle 21 (human rights diligence) which encourages external reporting on company practices that impact human rights. See www.telecomindustrydialogue.org.

[28] For example, civil society organisations in Canada, Hong Kong, Poland and USA have published reports or established websites that combine company statistics in one place or have completed comparative research across company reports.