CSISAC
Civil Society Information Society Advisory Council

May 3, 2021.

CSISAC Statement on Trusted Government Access to Personal Data Held by the Private Sector

CSISAC recognizes the importance of the work conducted by states and the OECD secretariat on Trusted Government Access to Personal Data Held by the Private Sector.[1] CSISAC acknowledges the impact of disproportionate government access to personal data held by the private sector on the economy and human rights. We appreciate that the 2020 December statement by the OECD Committee on Digital Economy Policy, announcing this discussion process, made explicit references to the need to provide safeguards around access to data and guarantee the protection of individual rights.[2]

This informal group will be tasked with developing draft high-level principles or policy guidance which will focus on the following seven issues: “the legal bases upon which governments may compel access to personal data; requirements that access meet legitimate aims and be carried out in a necessary and proportionate manner; transparency; approvals for and constraints placed on government access; limitations on handling of personal data acquired, including confidentiality, integrity and availability safeguards; independent oversight; and effective redress.” CSISAC supports these seven areas of work, though CSISAC would kindly ask OECD to provide more information on the participatory countries.

CSISAC notes that recommendations and principles are being developed on the basis of common practices. The OECD should acknowledge that there might be a tension between certains common practices on governments' access to data and countries’ adherence to their human rights obligations and Constitutions. The OECD should clarify whether it aims to identify common practices or to develop principles - that must be grounded in international human rights law. CSISAC would like to ensure that documents produced through this process are not presented as international principles that would run afoul of international human rights law and standards. CSISAC also calls for cautions to avoid condoning practices that may run contrary to many constitutions and States own human rights obligations.

Based on this information, CSISAC presents the following suggestions to guide the OECD’s work:

1https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm
2https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm

1. The OECD work must be based on human rights standards.

Trusted government access to data cannot happen if legislations and practices are not firmly rooted in international human rights standards. OECD members are obliged to protect and respect human rights. States' human rights obligations should be reflected in the ongoing discussions.

When it comes to rules for government access to data, CSISAC would like to highlight fundamental differences between countries with strong rules of law and democratic values versus non-democratic countries with poor human rights records. Furthermore, not all democratic countries apply the same level of protection for human rights. For example, while some States will allow access to some data in the absence of any judicial authority, others would not.[3]

If principles are developed on the basis of common practices, there is a risk of a race to the bottom in equaling practices across jurisdictions. These initiatives can potentially increase the scope of surveillance, disproportionate access, and contribute to the erosion of privacy in some countries. The OECD should acknowledge that there might be a tension between certains common practices on governments' access to data and countries' adherence to their human rights obligations. In fact, not all practices in place in democractic countries necessarily align with their human rights obligations.[4] If the OECD discusses common practices on access to data without addressing how these practices align with human rights obligations and the rule of law, the OECD may condone activities that harm rights. Alternatively, if the OECD chooses to focus on common practices, the title and presentation of the documents should reflect this reality and avoid adopting principles that may contradict obligations set under international human rights law.

If the OECD decides to focus on principles, we urge the informal drafting group to highlight and use in its works the "Necessary and Proportionate Principles".[5] These Principles are supported by over 250 civil society organisations and were built upon international agreed standards. These principles are specifically relevant to the matter discussed by the drafting group as they clarify how international human rights law applies in the digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques, including access to data by governments.

We further recommend the informal drafting group to make references to the CSISAC principles.[6] In particular, we draw the OECD's attention to the section on "protection of privacy and transparency" and recall the need for OECD countries to "adopt and enforce data protection

3The Canadian Supreme Court and the European Court of Human Rights have both recognised the need to protect individuals' online anonymity. In *Spencer*, the Court held that individuals can reasonably expect that the state will not seek to identify their otherwise anonymous online activity by asking their Internet Service Provider to voluntarily disclose their subscriber data. See *R v Spencer*, 2014 SCC 43, 2014 S.C.R. 212, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do and *Benedik v Slovenia*, App No 62357/14, April 24, 2018 http://www.bailii.org/eu/cases/ECHR/2018/363.html
To the contrary, the U.S. law allows voluntary disclosure of subscriber data to foreign governments.
4*See* Court of Justice of the EU, decisions on data retention practices in the EU, October 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf ; and ruling on EU-US data transfer mechanism, July 2020, https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5016067.
5https://necessaryandproportionate.org/principles/
6https://csisac.org/seoul.php

laws covering all sectors, both online and offline". Data protection laws are a core element of data governance models that contribute to the free flow of data with trust by empowering people, articulating rights and remedies structure, and providing legal certainty to public and private entities.

Finally, CSISAC stresses the need to address public independent oversight mechanisms. Having structures that enable accountability and public scrutiny on the conditions of access to data that are and will be adopted by governments increases the inclusion of the population in the decision making process. This measure requires that public authorities implement the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" and data protection principles as a whole in order to maintain people's trust.

2. The scope of the OECD work on government access to data for law enforcement and national security purposes should be clarified.

The current scope of the work on trusted government access to data may not cover all realities, challenges, and practices under which public authorities may gain access to private information. CSISAC recommends that the scope of work at the OECD should comprehensively consider government access to data held by private companies and provide clear recommendations based on human rights laws on what constitutes legitimate, necessary, and proportionate government access. There should also be clarification and limitation as to what categories of data held by companies, governments may be able to access in line with these principles.

In practice, in many countries, public authorities' access to data goes beyond activities conducted by law enforcement and intelligence services. Very often, public authorities request or gain access to information gathered by companies for commercial purposes to conduct their public security and national security objectives. In some cases, private companies also voluntarily hand over data to public authorities. While these practices may exist, it does not mean that they are in line with international human rights law and standards. As noted in your December statement, states' different practices on government access to data "may lead to undue restrictions on data flows resulting in detrimental economic impacts".[7] Yet if the objective is to facilitate more fluid cross-border access to data, this should also occur with a high level of protection rooted in international human rights standards. When surveillance activities are conducted through private companies, these practices not only harm rights and erode trust in government activities but they also undermine consumers' trust in businesses and harm the economy. Therefore, the development of clear limitations on practices and of safeguards based on human rights laws is to the interests of states, citizens and businesses.

During previous OECD debates on the use of vulnerability treatment, it was already established that in many countries, states and state-backed actors play a key role in surveilling illegitimate targets. As a result, surveillance and surveillance harms are not only derived from the actions of law enforcement and intelligence authorities[8]. In addition, a number of these practices are conducted outside proper legal framework, and/or with limited oversight and access to remedy. The work conducted at the OECD should reaffirm the need for a clear, predictable, and lawful process to be in place when private data is being accessed by public authorities.

7 https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm

8 The Offensive Role of governments, is one of the case studies that was described at the "Encouraging vulnerability treatment - overview for policy makers" OECD Paper that can be found at https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf?expires=1625689972&id=id&accname=guest&checksum=248A279389948B8CDED6F7AE270096CE

The discussion that OECD will address is particularly important in a context where access to data becomes ever more important in a digital society. It can raise challenges in a diverse range of public policy issues. The COVID-19 crisis highlights how often and easily, data, including health data, may be reused, including law enforcement purposes. In many countries, governments used emergency measures to weaken data protection regulations and to disproportionately increase access to personal data arguing a public health emergency.[9] Trusted data governance practices must reaffirm adherence to basic data protection principles of data minimisation and purpose limitation, including in the context of government access, and provide practical solutions regarding separation of powers.

We caution the OECD against the risk exacerbated by the ongoing global crisis of lowering existing and indispensable safeguards as states operate under urgency mechanisms. Rights must be even more protected during emergency situations, anything else would lead to unjustified harm of human rights. The surveillance of vulnerable populations by state and private actors alike with the excuse of determining and facilitating their access to social benefits is one of the many examples of new and worrisome developments that have important impacts on people's rights,[10] as the UN rapporteur for extreme poverty reported in 2019.[11] Increasingly, access to data by governments goes beyond law enforcement and intelligence purposes and it is not limited to purposes linked to their public duties or powers. The OECD work should take into account the fact that states may be buying or otherwise reaching public-private agreements to share large amounts of data from private sources or seeking the capacity to mix public data silos. These agreements and the increasing dependence of states to rely on private actors and the data they collect to conduct their public roles, whether in the area of security, health, or the economy, should be addressed by the OECD.

3. The OECD work should promote access to remedy, robust oversight and transparent processes.

CSISAC notes that the current scope of work of the informal drafting includes discussions on "independent oversight and effective redress". We strongly support ensuring that conditions on access to data should include mechanisms for independent oversight and access to effective redress mechanisms that should be directly available for people in cases of abuse or violations of rights. A recent paper comparing the legal frameworks on access to data by governments under law enforcement and intelligence authorities in eight countries of Latin America, shows that these countries have weak frameworks for the protection of human rights.[12]

9 In Colombia, the Data Protection Authority issued an administrative order that authorises business, and particularly mobile network operators, to share their client's data with authorities: https://web.karisma.org.co/useless-and-dangerous-a-critical-exploration-of-covid-apps-and-their-human-rights-impacts-in-colombia/.
Other examples were collected by Privacy International: https://privacyinternational.org/examples/tracking-global-response-covid-19

10 For instance, in Colombia, public authorities are using banking data handed by data brokers to verify the deservedness of social security: https://web.karisma.org.co/experimenting-with-poverty/
In the UK, the Home Office uses purchasing data to spy on the habits of asylum seekers: (https://privacyinternational.org/explainer/4425/what-aspen-card-and-why-does-it-need-reform)

11 https://www.ohchr.org/EN/Issues/Poverty/Pages/DigitalTechnology.aspx

12 *A Human Rights Legal Framework for Communications Surveillance in Latin America, Argentina, Brazil, Chile, Colombia, Mexico, Panama, Paraguay, and Peru*, (executive summary in English) can be found at https://www.alsur.lat/en/report/executive-summary-human-rights-legal-framework-communications-surveillance-latin-america. See also *When Law Enforcement Wants Your Private Communications, What Legal Safeguards Are in Place in Latin America and Spain?*

The OECD should further take into consideration the breaches of access to information laws and increased unjustified secrecy around law enforcement and intelligence activities. These practices may impact the level of oversight that authorities and external experts can exercise over government practices. Governments have repeatedly disregarded domestic laws on access to information, either by failing to respond to requests or through unsatisfactory responses, which do not address the questions raised.[13] In some institutions, this problem of transparency deepens when requests for information are denied on the basis that it would "compromise the integrity or security of investigation activities or that of its agents". This argument is commonly and increasingly used for most requests, thus applied in a generalised way and based on incorrect interpretations of the secrecy laws. A recent decree in Brazil has further increased the use of this flawed justification.[14]

In addition to guaranteeing transparency, access to effective remedy, and oversight mechanisms, we recommend OECD to discuss notification obligations by private companies when their data is disclosed to law enforcement. We also recommend that companies provide auditable tools to review access requests and mandatory reporting on data access demands. Similarly, we call on the OECD to include references to core data protection principles promoted and advanced in your own guidelines, including data minimisation principles, purpose limitation principles, limited data retention, and to promote data protection impact assessments. CSISAC also calls for requirements that public policies should consider that the safeguards to protect human rights include constant revisions through dynamic and transparency review mechanisms, with ex-ante and ex-post assessments. Finally, the documents to be produced by the drafting group should mention what are the necessary and proportionate protocols to deliver data to authorities during investigations. For instance, this discussion could provide clarity regarding the categories of data that may be requested, how and when, by which authorities and under which oversight mechanism.

While disproportionate access to data hurts rights and the economy, data protection rights empower people and provide a basis for trusted free flow of data internationally. It is therefore crucial for the OECD to acknowledge the role of national and regional data protection laws in bringing trust, legitimacy and certainty in rules on access to data that shall be respected by private and public sector authorities.

https://www.eff.org/deeplinks/2021/02/when-law-enforcement-wants-your-private-communications-what-legal-safeguards-are; *Despite Progress, Metadata Still Under "Second Class" Protection in Latam Legal Safeguards,* https://www.eff.org/deeplinks/2021/02/despite-progress-metadata-still-under-second-class-protection-latam-legal

13*Latin American Governments Must Commit to Surveillance Transparency* https://www.eff.org/deeplinks/2020/10/latin-american-governments-must-commit-surveillance-transparency

14https://www.bbc.com/portuguese/brasil-46992821 Summary: in January 2019, the Brazilian federal government published a decree that expanded the categories of public agents capable of classifying information as top secret, being able to keep it confidential for up to 25 years. Signed by interim president Hamilton Mourão, the decree amends the Access to Information Law, allowing occupants of commissioned positions - who may be politically appointed - to classify information as top secret in cases where its disclosure "threatens the security of society or the state."
To limit the application of the law of access to information, public authorities conduct practices that include a 'mental ranking' of those who introduce a request to access a given information: https://sao-paulo.estadao.com.br/noticias/geral,gestao-doria-dificulta-acesso-a-dados-e-viola-lei-de-acesso-a-informacao,70002075921

4. The OECD should ensure diversity of perspective in the research, gathering and analysis of the evidence used for this work.

Principles produced by OECD become important references around the world. Therefore, OECD should ensure that the research and evidence provided to the informal drafting group to assist with their work comes from diverse sources and expertise.

CSISAC cautions the OECD overdrawing conclusions solely based on experiences from developed countries. Many developing countries will have a very different social, institutional, political, and economic landscape and it should be taken into account in the building of these principles.

CSISAC further calls on the OECD to engage with civil society actors throughout the drafting process and provide several opportunities to access the document and comments upon it before concluding the documents. This inclusive process would allow for civil society to provide concrete examples of the impact of government access to private data on human rights.

CSISAC looks forward to continuing engaging with the OECD on these important discussions and to provide comments and inputs to documents produced by the informal drafting group.