GOVERNMENT ACCESS TO DATA PROCESSED
IN A PUBLIC CLOUD ENVIRONMENT

CHAPTER 11

CLOUD AND GOVERNMENT ACCESS

Andrea Raab-Gray*

* Disclaimer: the opinions and views expressed in this contribution are the author's own and do not necessarily represent those of the Federal Ministry of European and International Affairs of the Republic of Austria.

States around the globe have in place domestic laws authorizing governments to require service providers to disclose to them manifold types of data created by or relating to a customer, in the interest of national security and/or for use in criminal proceedings. The often-cited rationale underlying such legislation is a growing use of digital technologies, including cloud computing, for illicit purposes.[1] Yet, even if only as a side effect, many of these legislations also enable governments to compel the disclosure of data pertaining to action of Humanitarian Organizations, processed in a public cloud environment. Such data could encompass data that Humanitarian Organizations generate, collect or exchange with others, including the contents of communications within the organization, with their partners or persons benefiting from their action. Data subject to disclosure also often include meta, location and traffic data, that is, data about the communications other than their contents, such as data about the recipient of a communication, the duration of a call and the like.[2] For purposes of brevity, this chapter will refer to such content, meta, location and traffic data together as "Humanitarian Data".

In terms of relevance of Humanitarian Data to States, it is important to understand that Humanitarian Organizations often fulfil their mandates in a Neutral, Impartial and Independent manner. As such, several such organizations provide assistance to and generally conduct dialogue with all sides to an armed conflict or other crisis. This may include non-State actors and individuals which States might designate as "terrorists" in relevant legislative frameworks. In granting impartial Humanitarian Organizations a right of initiative, international humanitarian law for instance accommodates – and indeed endorses – this. This right entails that impartial Humanitarian Organizations may offer their humanitarian activities to parties to international and non-international armed conflicts, regardless of how a conflict may be characterized under counterterrorism or sanctions regimes.[3] Thus, Humanitarian Data can be of interest to governments for purposes of counterterrorism action and criminal proceedings.

In selecting technology, and particularly Cloud Services, Humanitarian Organizations should therefore consider legal and operational consequences stemming from legislations allowing governments to require disclosure of data from service providers, including those processing Humanitarian Data. This chapter seeks to inform Humanitarian

1 See for example: US Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law around the World: The Purpose and Impact of the CLOUD Act*, White Paper, US Department of Justice, Washington, DC, April 2019: www.justice.gov/dag/page/file/1153436/download.

2 For further information on the importance of metadata for Humanitarian Organizations, see ICRC and Privacy International, *The Humanitarian Metadata Problem*.

3 See Common Article 3 to the 1949 Geneva Conventions, as well as Common Articles 9/9/9/10. For further information on this, see Tristan Ferraro, "International humanitarian law, principled humanitarian action, counterterrorism and sanctions: Some perspectives on selected issues", *International Review of the Red Cross*, Vol. 103, No. 916/917, 2021, pp. 109–155.

Organizations in their reflections: Section 11.1 maps legislations that, even if only as a by-product, allow governments to require service providers to disclose Humanitarian Data for purposes of national security and/or criminal proceedings. Section 11.2 outlines criteria for Humanitarian Organizations to consider when assessing the impacts such disclosure can have on persons benefiting from their action, and organizations' operations. Finally, Section 11.3 provides guidance as to the legal avenues Humanitarian Organizations could take in mitigating the risk of disclosure of Humanitarian Data if they choose to process Humanitarian Data in a public cloud environment.[4]

11.1 MAPPING LEGISLATIONS ALLOWING GOVERNMENTS TO REQUIRE SERVICE PROVIDERS TO DISCLOSE HUMANITARIAN DATA

Humanitarian Organizations should take into account legislations that allow governments to compel service providers to disclose to governments Humanitarian Data for purposes of national security and/or criminal proceedings, in selecting technology, and particularly when:

- considering whether and which data to process in a public cloud environment; and
- selecting cloud service providers.

Propelled by the increasing use of digital technologies, including Cloud Services, for illicit purposes,[5] the legislations discussed in this chapter are not as such intended to target specifically Humanitarian Data. However, these legislations do not exclude

4 This chapter does not address forms of "illegal access", such as hacking without any legal basis. This is because illegal access is not necessarily cloud-specific and raises broader questions both in relation to legal and cyber security responses. See for instance Massimo Marelli, "Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation", *International Review of the Red Cross*, Vol. 102, No. 913, April 2020, pp. 367–387: https://doi.org/10.1017/S1816383121000151. Equally, this chapter does not discuss so-called cloud extraction, a forensic analysis of user data which is stored on Third Party servers, typically used by device and application manufacturers to back up data. Increasingly used by law enforcement, this new trend raises similar concerns for Humanitarian Organizations to the legislations discussed in this chapter. For further information, see Privacy International, "Cloud Extraction", Privacy International, 9 May 2022: https://privacyinternational.org/learn/cloud-extraction; Privacy International, "Are UK Police Accessing Your Cloud Apps?", Privacy International, 1 April 2020: http://privacyinternational.org/report/3551/are-uk-police-accessing-your-cloud-apps; Privacy International, "Secret Tech Lets Governments Collect Masses of Data from Your Apps", Privacy International, 6 January 2020: http://privacyinternational.org/node/3323.

5 See for instance: European Commission, "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters", COM/2018/225 final, 17 April 2018: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN.

Humanitarian Data from their scope, either: indeed, these legislations do not generally contain "humanitarian exemption clauses" explicitly excluding Humanitarian Data. On the contrary, oftentimes legal requirements authorizing governments to require disclosure of data from service providers squarely apply to Humanitarian Data, as will be shown below.

Disclosure requests for Humanitarian Data addressed to service providers differ as compared to disclosure requests for such data served on Humanitarian Organizations themselves. Where a Humanitarian Organization receives such a request itself, it is in a position to evaluate how to respond to this request, in light of its mandate and policies. Should it decide not to accede to a disclosure request, it may resort to remedies enshrined in national law to oppose disclosure. In addition, a Humanitarian Organization might be able to invoke privileges and immunities which they may enjoy under national and/or international law (see also Section 11.3 – Mitigating the risk of disclosure of Humanitarian Data processed in a public cloud environment, further below). This is irrespective of where data are hosted, be it in a private or public cloud environment. Yet, when providers receive disclosure requests from State authorities, Humanitarian Organizations are dependent on how the provider will respond to such a request, for instance whether they will inform the Humanitarian Organization of a disclosure request (provided they are legally permitted to do so), and whether they will raise legal defences to oppose the request.[6]

This chapter draws on illustrative examples of relevant legislations in the United States, the United Kingdom and the European Union. It should however be noted that other States too have adopted legislation enabling them to compel service providers to disclose customer data – including potentially data of Humanitarian Organizations – for purposes of national security and/or criminal proceedings.[7]

11.1.1 LEGAL FRAMEWORKS ALLOWING GOVERNMENTS TO COMPEL SERVICE PROVIDERS TO DISCLOSE HUMANITARIAN DATA FOR PURPOSES OF NATIONAL SECURITY

Several States have adopted legislation providing governments with legal avenues to compel service providers under their jurisdiction to disclose data for purposes of

6 See also Section 10.9 – Privileges and immunities and the cloud, on the legal measures to be taken by Humanitarian Organizations to ensure the effectiveness of privileges and immunities in protecting data processed in a cloud environment.

7 See for instance the Parliament of Australia, Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (2020): https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbillhome%2Fr6511%22. See also European Data Protection Board (EDPB), "Government Access to Data in Third Countries", EDPS/2019/02-13, November 2021: https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf.

national security. Thus, by choosing cloud service providers under those States' jurisdiction, Humanitarian Organizations should be aware that their data might be subject to disclosure for national security purposes.

A well-known example of such legislation is the US PATRIOT Act, enacted in October 2001 in response to the attacks on the World Trade Center.[8] It allows the US government to require service providers under US personal jurisdiction[9] to disclose certain data to them. It follows that, when a Humanitarian Organization onboards services of a US service provider, its data might come within the scope of the PATRIOT Act and might be vulnerable to disclosure requests under that Act.

Of particular interest for Humanitarian Organizations contemplating the use of Cloud Services are the PATRIOT Act's regimes on orders made under the Foreign Intelligence Surveillance Act (FISA), as well as on National Security Letters.[10] Under the FISA, the US government is authorized to:

- obtain a secret court order requiring Third Parties, such as cloud service providers, to hand over any records or other "tangible thing" if deemed "relevant" to an international terrorism, counterespionage, or foreign intelligence investigation;[11] and
- issue orders requiring, for instance, cloud service providers under US personal jurisdiction to disclose communications data of specific non-US persons located outside the United States to obtain specified types of foreign intelligence information, upon authorization by an independent court, the FISA Court.[12]

8 Specifically, to facilitate the investigation of terrorism crimes, the Act amended pre-existing laws by extending the application of surveillance tools to terrorism investigations, and expanded their scope. See on this and on the PATRIOT Act more generally: US Department of Justice, "The USA PATRIOT Act: Preserving Life and Liberty", n.d.: www.justice.gov/archive/ll/what_is_the_patriot_act.pdf; American Civil Liberties Union, "Surveillance under the USA/PATRIOT Act", n.d.: www.aclu.org/other/surveillance-under-usapatriot-act; Greenberg Traurig LLP, "Schrems II – U.S. Legislation", Memorandum, 12 February 2022: https://slmmicrosoftrijk.nl/wp-content/uploads/2022/02.

9 See for instance Daniel Levin and Jacqueline L. Chung, "Patriot Act Subpoenas: Reinvigorated and Reaching across Borders", White & Case LLP, n.d.: www.whitecase.com/insight-alert/patriot-act-subpoenas-reinvigorated-and-reaching-across-borders.

10 While the number of requests for FISA orders is relatively low, National Security Letters have been used more frequently. For 2020 statistics, see Joseph Gaeta, "Letter to Nancy Pelosi", 30 April 2021: www.justice.gov/nsd/nsd-foia-library/2020_fisa/download.

11 Brennan Center for Justice, "Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs", accessed 27 November 2022: www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf. See also: "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001", Pub. L. No. 107-56, § 215 (2001): www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf; 50 U.S.C. §1804(a)(6)(B).

12 See "An Act to Authorize Electronic Surveillance to Obtain Foreign Intelligence Information", Pub. L. No. 95-511, § 702 (1978), www.congress.gov/bill/95th-congress/senate-bill/1566. According to the Brennan Center for Justice at New York University, this section has also been cited as the legal

The FISA Court has authorized the collection of both metadata and content of communications pursuant to section 702 under at least some circumstances.[13] Section 702 has been applied to both data in transit and data at rest.[14]

By virtue of National Security Letters, the Director of the Federal Bureau of Investigation (FBI) and other high-ranking FBI officials can require, for example, cloud service providers to disclose subscriber information and toll billing records information, or electronic communication transactional records that are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.[15] It follows that National Security Letters cannot be used to obtain any data about the content of communications.

Humanitarian Data might indeed be "relevant" to the purposes outlined above. For instance, to fulfil their mandate in an impartial and neutral manner, some Humanitarian Organizations might conduct dialogue with groups designated as "terrorist", or furnish humanitarian assistance to persons under the control of such groups. If these organizations choose to process data pertaining to this dialogue in a public cloud environment, some of these data might be subject to disclosure under the PATRIOT Act.

In Europe, case law of the European Court of Justice (CJEU) is instructive in delineating the contours of EU Member States' powers to require service providers to retain, in particular, traffic and location data for purposes of government access. While the case law of the CJEU does not specifically concern cloud computing, the author nevertheless considers it relevant for the discussion at hand: it allows conclusions to be drawn about the general approach towards balancing national security considerations and rights in Europe. As such, it cannot be excluded that the said criteria are equally applied in a cloud context.

In the *Watson* and *Privacy International* cases, the CJEU had to consider, amongst other legislations, UK law allowing authorities to require certain service providers to retain and grant access to certain metadata.[16] In both cases, the Court held that

justification for PRISM, a computer network facilitating access to data processed by nine leading US Internet companies, including Google, Facebook, Skype and Apple: Brennan Center for Justice, "Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs".

13 Stephen I. Vladeck, "Expert opinion on the current state of U.S. surveillance law and authorities", in *Conference of Independent Data Protection Supervisors of the Federal Government and the Länder*, 2021, 2: www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.

14 Ibid., 4.

15 18 U.S.C. § 2709.

16 Joined Cases C-203/15 and C-698/15 (*Tele 2 Sverige* and *Watson*), Judgment (Grand Chamber), 21 December 2016; Case C-623/17 (*Privacy International*), Judgment (Grand Chamber), 6 October 2020. In *Privacy International*, for instance, the CJEU was asked to determine which requirements apply to an

national legislation which provides for the general and indiscriminate retention and disclosure to authorities of all traffic and location data of all subscribers relating to all means of electronic communication is incompatible with EU law.[17] Yet, the Court also stated that "in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combatting such activities".[18] As such, the criteria set out by the Court do not *per se* target Humanitarian Data, but they also do not exclude such data. On the contrary, where a Humanitarian Organization in fulfilling its mandate conducts dialogue with certain non-State actors, location and traffic data pertaining to such dialogue *might* indeed be considered to contribute to combatting "terrorist activities".

Moreover, Humanitarian Organizations might not even be aware that their data are being sought. For instance, under the PATRIOT Act, US government authorities can impose non-disclosure obligations, whereby service providers are prohibited from informing any Third Party – including Humanitarian Organizations as customers – about the National Security Letter or FISA order.[19]

Finally, in choosing to process Humanitarian Data in a public cloud environment, Humanitarian Organizations should also consider potential risks stemming from interception by security authorities. In the seminal *Big Brother Watch* case, the European Court of Human Rights examined, amongst other issues, the compatibility with Article 8 of the European Convention on Human Rights of warrants issued under the UK Regulation for Investigatory Powers Act 2000 (RIPA), allowing for bulk interception by security agencies of both content and communications data for purposes of national security.[20] In so doing, the Court emphasized the need for clarity of such laws in relation to grounds for bulk interception, applicable procedure, limitations and safeguards.[21] The Court also considered that the same safeguards

order by authorities to a service provider to disclose to them bulk communications for national security purposes under the UK Regulation for Investigatory Powers Act 2000 (RIPA) and the UK Telecommunications Act 1984. On data retention, see also Joined Cases C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and ors*), 6 October 2020.

17 *Watson*, para. 112; *Privacy International*, para. 81.

18 *Watson*, para. 119. See also *Privacy International*, para. 78.

19 50 U.S.C 1861(d); 18 U.S.C § 2709(c).

20 *Big Brother Watch and others v. United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15, Grand Chamber, Judgment, 25 May 2021. For a similar case, see *Centrum för rättvisa* v. *Sweden*, Application no. 35252/08, Grand Chamber, Judgment, 25 May 2021.

21 *Big Brother Watch*, para. 361. For a summary of other parts of the judgments,see Marko Milanovic, "The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum För Rättvisa", EJIL: Talk! (blog), 26 May 2021: www.ejiltalk.org/the-grand-

should apply to the collection and Processing of communications data and metadata, not just the content of communications.[22] Importantly, the Court did not define any criteria which might exclude Humanitarian Data from the scope of bulk interception.[23] The UK RIPA was replaced by the UK 2016 Investigatory Powers Act. This piece of legislation too allows for a bulk interception warrant for "content" of communications and/or "secondary data", including certain data which may be used to identify any person or the location of any person, event or thing, if this is necessary in the interests of national security, amongst other grounds, without explicitly excluding Humanitarian Data.[24]

While the *Big Brother Watch* case again does not specifically concern cloud computing, the author considers it relevant for the same reasons as set out above in relation to the case law of the CJEU.

11.1.2 LEGAL FRAMEWORKS ALLOWING GOVERNMENTS TO COMPEL SERVICE PROVIDERS TO DISCLOSE DATA FOR PURPOSES OF CRIMINAL PROCEEDINGS

One of the most prominent examples of such legislations is the US CLOUD Act. The first part of the CLOUD Act clarifies that:[25]

normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa. While the *Big Brother Watch* case in particular did not concern obligations on the service provider to provide data to national authorities, it is crucial in showcasing the extent of deference courts have paid to national security interests.

22 *Big Brother Watch*, paras. 342, 363–364.

23 Ultimately, the Court found that the bulk interception regime of the RIPA breached privacy obligations under the Convention, *Id*, paras. 424–427. While some human rights organizations have hailed the judgment a landmark victory, other commentators have criticized the decision as normalizing mass surveillance and bulk interception, highlighting that the Court considered those mechanisms as "valuable" and of "vital importance" to the security of Member States of the Council of Europe. See Milanovic, "The Grand Normalization of Mass Surveillance", setting out different positions taken.

24 See sections 136 *et seqq.* of the 2016 Investigatory Powers Act. Note in this regard the case of *Privacy International v. Investigatory Powers Tribunal, [2021] EWHC 27 (Admin)*, 8 January 2021. Privacy International explain that, in that case, the UK High Court held that section 5 of the Intelligence Services Act (ISA) 1994 does not permit the security and intelligence services to rely on non-specific warrants – otherwise known as general warrants – to authorize their wide-ranging hacking and property interference powers. Thematic warrants are general warrants covering an entire class of property, persons or conduct, such as "all mobile phones used by a member of a criminal gang", without specifying the names or locations of the members. Privacy International, "Q&A: PI Case – UK High Court Judgment on General Warrants and Government Hacking Explained", Privacy International, 8 January 2021: http://privacyinternational.org/long-read/4361/qa-pi-case-uk-high-court-judgment-general-warrants-and-government-hacking-explained. It remains to be seen if this judgment will have any impact on the interpretation of the IPA.

25 For more information, see also US Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law around the World*; Vladeck, "Expert opinion on the current state of U.S. surveillance law and authorities", 13; Greenberg Traurig LLP, "Schrems II – U.S. Legislation", 12 February 2022, 9; Swiss

- US authorities may compel the disclosure of content *and* traffic data over which a service provider under US personal jurisdiction has "possession, custody or control":[26]
  - for purposes of certain criminal proceedings;[27]
  - irrespective of where the data are located.[28]

There is nothing in this first part of the CLOUD Act that exempts Humanitarian Data from its scope of application, nor are there any other limitations within the CLOUD Act that would implicitly exempt such data.

It follows that, if Humanitarian Organizations choose a service provider under US personal jurisdiction to process Humanitarian Data, these data might be vulnerable to requests for disclosure by US authorities, to the extent the US service provider has "custody, possession or control" over such data. The Act does not define the notions of "custody, possession or control", and, at the time of writing, it remains to be seen

Federal Department of Justice, "Bericht zum US CLOUD Act", 17 September 2021: www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html.

26 US Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law around the World*, 8. It is noteworthy that the DoJ advised that CLOUD Act orders should be subsidiary measures, in that "prosecutors should seek data directly from the enterprise, if practical, and if doing so will not compromise the investigation. Therefore, before seeking data from a provider, the prosecutor, working with agents, should determine whether the enterprise or the provider is the better source for the data being sought": 17.

27 See 18 U.S.C, §2703(b).

28 Legal discourse focused on the question of whether the CLOUD Act triggered improper extraterritoriality of sovereign acts. See for example: Johannes Thumfart and Paul De Hert, "Both the US's Cloud Act and Europe's GDPR Move Far Beyond Geography, but Will Not Solve Transatlantic Jurisdictional Conflicts", Just Security, 4 June 2018: www.justsecurity.org/57346/uss-cloud-act-europes-gdpr-move-geography-solve-transatlantic-jurisdictional-conflicts. Everything started with the *Microsoft* litigation: In December 2013, federal law enforcement agents were granted a warrant requiring Microsoft to disclose all emails and other information associated with the account of one of its customers. (US Supreme Court, *United States v. Microsoft Corporation*, 584 U. S. (2018), p. 1.) Microsoft moved to quash the warrant, arguing that the account's email contents were stored solely in Microsoft's data centre in Ireland, i.e. outside the reach of US law. (Ibid., p. 2.) The question hence facing US courts was whether the data location outside the United States would pose an obstacle to enforcing the warrant, constituting improper extraterritorial application of US law. Microsoft and the US government litigated this question in various instances, and courts' opinions differed: While the Magistrate Judge denied Microsoft's motion, the Court of Appeals considered that requiring Microsoft to disclose the electronic communications in question would be an unauthorized extraterritorial application of the relevant US Act that served as a legal basis of the warrant. (*In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 829 F. 3d 197, 205, 222 (CA2 2016).) Ultimately, the matter came before the US Supreme Court, which however vacated the review, as the US CLOUD Act had meanwhile entered into force which resolved the matter, by allowing US authorities to require disclosure from US service providers even if data are located abroad. (US Supreme Court, *United States v. Microsoft Corporation*, pp. 2–3.)

how authorities and courts will construe those terms in the context of the CLOUD Act.

Further to this, the US government can impose a non-disclosure obligation on the service provider under certain circumstances.[29] This means that the service provider may be prohibited from notifying the Humanitarian Organization of the existence of a request for its data.

EXAMPLE (SIMPLIFIED):
In fulfilling its mandate in a manner neutral and impartial, and to secure access to affected populations and provide them with humanitarian assistance, the Humanitarian Organization HO maintains dialogue with the group G, and its leader L. Group G is listed as a "terrorist" group under relevant legislation. HO stores the contents of this dialogue in a public cloud environment. The Cloud Services are provided by service provider SP, incorporated in New York (United States). Data are stored in Europe.

Under the US CLOUD Act, US authorities could have the power to legally oblige SP to disclose such data for purposes of certain criminal proceedings against L. SP might be prohibited from informing HO of this request. On blocking statutes and the impact of privileges and immunities, see Section 11.3 – Mitigating the risk of disclosure of Humanitarian Data processed in a public cloud environment, below.

Humanitarian Organizations should also bear in mind that choosing a US service provider might also allow other States to require disclosure of humanitarian content and traffic data from that service provider, for purposes of criminal proceedings.

This is because the second part of the CLOUD Act authorizes the US government to enter into so-called executive agreements with other countries, allowing one State party to require the disclosure of certain content and traffic data from service providers under the other party's jurisdiction, and vice versa, for purposes of preventing, detecting, investigating or prosecuting serious crime, including terrorism.[30] There is nothing in this second part of the CLOUD Act that exempts Humanitarian Data from its scope of application. The prime example for this is the UK/US

29 18 U.S.C, §2703(b), §2705.

30 18 U.S.C. §2523(b)(4)(D)(i). Disclosure orders must not intentionally target US persons. This term is defined as "a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States". 18 U.S.C. §2523(a)(2).

agreement, concluded under the second part of the CLOUD Act, and the UK Crime (Overseas Production Order) Act.[31]

The UK's equivalent to the second part of the CLOUD Act is the Crime (Overseas Production Order) Act, which received royal assent in February 2019. This law:[32]

- enables UK law enforcement agencies[33] to apply for a court order from a judge with extraterritorial effect ("Overseas Production Order");
- to obtain electronic data directly from service providers operating or based outside the UK but "in the possession or control" of the data sought;
- for purposes of criminal investigations and prosecutions of indictable offences or terrorist investigations;
- where a designated international cooperation arrangement with the State in which the service provider operates, is already in place.

There is nothing that explicitly exempts Humanitarian Data from the scope of the Act, although there is one exemption to the data that can be obtained via an Overseas Production Order that might be relevant for some Humanitarian Organizations: electronic data means data stored electronically and thus encompasses content and telecommunications data hosted in a public cloud environment.[34] Yet, information subject to legal privilege, such as certain communications between a client and their legal counsel, as well as personal records which are confidential information cannot be obtained via an Overseas Production Order.[35] Personal records which are confidential information include Health Data as well as data pertaining to counselling or assistance given, or to be given, to an individual for purposes of their personal welfare by any voluntary organization, if that record was created, amongst others, in circumstances giving rise to an obligation of confidence owed to the individual.[36] This latter exemption could in very rare cases encompass some data pertaining to Humanitarian Action undertaken by a Humanitarian Organization. Yet, the Act does not include any explicit exemption from its scope of application for data pertaining to Humanitarian Action.

Only electronic data that are likely to be of substantial value to these proceedings or investigations can be required to be disclosed under an Overseas Production Order.[37]

31 Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, 3 October 2019: www.justice.gov/dag/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern-ireland.

32 Crime (Overseas Production Order) Act, sections 1, 2 and 4.

33 These include, *inter alia*, constables, prosecutors, and other persons specified in regulations made by the Secretary of State. Crime (Overseas Production Order) Act, section 2.

34 See Crime (Overseas Production Order) Act, section 3(2).

35 Crime (Overseas Production Order) Act, section 3(3).

36 Crime (Overseas Production Order) Act, sections 3(7) and 3(8).

37 Crime (Overseas Production Order) Act, section 4(5).

As noted above, to fulfil their mandate in an impartial and neutral manner, some Humanitarian Organizations might conduct dialogue with groups designated as "terrorist", or furnish humanitarian assistance to persons under the control of such groups. As such, it cannot be excluded that those Organizations may store information about that dialogue in a cloud environment, and that such information might indeed be of "substantial value" in terrorist investigations.

Premised on the second part of the CLOUD Act and the Crime (Overseas Production Order) Act, the US/UK agreement does not contain any express exemptions for Humanitarian Data. Therefore, such data can in principle also be required from service providers, unless one of the limitations contained in the agreement is applicable.

EXAMPLE 1 (SIMPLIFIED):
In fulfilling its mandate in a manner neutral and impartial, and to secure access to affected populations and provide them with humanitarian assistance, a Humanitarian Organization (HO) maintains dialogue with group G, and its leader L. Group G is listed as a "terrorist" group under relevant legislation. HO stores the contents of this dialogue in a public cloud environment. The Cloud Services are provided by Service Provider (SP), incorporated in New York (United States).

Under the US/UK agreement, UK authorities may require SP to disclose HO's data for purposes of "terrorist investigations", by presenting a duly approved court order to SP. Unless excluded from the scope of the agreement, SP must provide the information sought to UK authorities. On access by US authorities, see above, previous example.

EXAMPLE 2 (SIMPLIFIED):
In fulfilling its mandate in a manner neutral and impartial, and to secure access to affected populations and provide them with humanitarian assistance, the Humanitarian Organization HO maintains dialogue with group G, and its leader L. Group G is listed as a "terrorist" group under relevant legislation. HO stores the contents of this dialogue in a public cloud environment. The Cloud Services are provided by Service Provider (SP UK), incorporated in the UK.

Under the US/UK agreement, US authorities may require SP UK to disclose HO's data for purposes of "terrorist investigations", by presenting a duly approved warrant to SP UK. Unless excluded from the scope of the agreement, SP UK must provide the information sought to US authorities.

As far as is public knowledge, the only other agreement concluded at the time of writing which is similar to the UK/US agreement is an agreement between the United States and Australia.[38]

Humanitarian organisations should also be aware that the EU has adopted adopting legislation similar to the CLOUD Act and Crime (Overseas Production Order) Act, namely the e-Evidence Regulation, which will apply in full from 18 August 2026. The Regulation establishes a regime whereby law enforcement authorities ("LEAs") in one EU Member State will be able to issue legally-binding demands for certain data from certain categories of service providers (namely providers of electronic communications services, domain name and IP registration services, and information society services that enable users to communicate or store data) that are established or have a legal representative in a different EU Member State, or demand such service providers to preserve such data.[39]

On a broader European level, Humanitarian Organizations should note that the Committee of Ministers of the Council of Europe has adopted a Second Additional Protocol to the Convention on enhanced cooperation and the disclosure of electronic evidence. The Protocol aims to:

> *further enhance co-operation on cybercrime and the collection of evidence in electronic form of any criminal offence for the purpose of specific criminal investigations or proceedings through additional tools pertaining to more efficient mutual assistance and other forms of co-operation between competent authorities; cooperation in emergencies; and direct co-operation between competent authorities and service providers and other entities in possession or control of pertinent information.*[40]

To this end, the Protocol foresees for instance that a State Party may issue an order directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the subscriber information is needed for the issuing Party's specific criminal investigations or proceedings.[41]

38 Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime, 15 December 2021: www.justice.gov/dag/cloud-act-agreement-between-governments-us-and-australia. For more resources, see Department of Justice, Cloud Act Resources, available at: Cloud Act Resources (justice.gov).

39 Lisa Peets, Marty Hansen, and Paul Maynard, "The EU E-Evidence Package Is Published in the Official Journal," Inside Global Tech, August 23, 2023, www.insideglobaltech.com/2023/08/23/the-eu-e-evidence-package-is-published-in-the-official-journal/#:~:text=In%20summary%2C%20the%20Regulation%20establishes,domain%20name%20and%20IP%20registration.

40 Preamble of the Protocol.

41 See Art. 7(1) of the Protocol.

11.2 IMPACTS OF COMPELLED DISCLOSURE ON HUMANITARIAN ACTION AND PERSONS BENEFITING FROM IT

In considering whether the legislations explained in the previous chapter pose any challenges to a Humanitarian Organization, one should take into account the impacts the disclosure of Humanitarian Data can have on:

- persons benefiting from action of a Humanitarian Organization; and
- operations of the Humanitarian Organization.

As regards the impacts on persons benefiting from Humanitarian Action, much depends on the services the Humanitarian Organization provides, and the type of data it collects from individuals.

EXAMPLE:
In fulfilling its mandate, a Humanitarian Organization might provide health services to survivors of sexual violence, and obtain their medical data as well as information about the circumstances of the sexual violence committed against them. The Humanitarian Organization stores this information in a public cloud environment. A State might seek to obtain data about this survivor when investigating sexual violence crimes in a given context, on the basis of territorial, personal or universal jurisdiction.

The compelled disclosure of medical data and data about the circumstances of the sexual violence for purposes of criminal proceedings can cause harm to the survivor themselves. In the first place, it takes away the agency of the survivor to themselves decide whether to provide this information to authorities. Second, in many communities, rape is still stigmatized, and survivors would be ostracized if it were known that sexual violence was committed against them. Thus, the compelled disclosure of a survivor's data and the subsequent use in legal proceedings can compound the harms facing survivors.

The impacts that compelled disclosure can have on the operations of a Humanitarian Organization depend on their mandate and working modalities. Some Humanitarian Organizations interact regularly with governments and pass on information to them in favour of an individual, for instance to facilitate the granting of rights or a legal status to that individual. By contrast, other Humanitarian Organizations act on a strictly confidential basis and would not share with governments the contents of their dialogue with States, individuals or other actors, since this may be an essential working modality required to build trust and access areas affected by armed conflicts and other situations of violence. For some organizations, this working modality has been endorsed and indeed safeguarded by the international community, and considered as a prerequisite for affected persons to have access to essential humanitarian

services.[42] Humanitarian Organizations should bear in mind that the difficulty with the legislations examined above is that they allow authorities to require service providers directly to disclose data of Humanitarian Organizations. Thereby, they do not generally leave space to take into account the differing relations Humanitarian Organizations entertain with law enforcement, and the particularities of Humanitarian Organizations' distinct mandates and practices risk being lost in translation, which can lead to harm for the organization itself, and, ultimately, the people it serves.

Moreover, in considering impacts of compelled disclosure on their operations, Humanitarian Organizations should also consider how the fact that Humanitarian Data might be used for purposes other than those for which they were provided might impact on the trust that stakeholders vest in the organization:[43]

- Persons benefiting from Humanitarian Action might not wish to engage with a Humanitarian Organization and thus not receive essential humanitarian services or aid that could improve their lives and livelihoods, if they do not have confidence that their data will be used exclusively for the purposes for which they were provided, and will only be processed in a Neutral, Impartial and Independent manner.
- The same applies to States: if States in which Humanitarian Organizations operate consider that there is a risk that data which these organizations collect in or receive from a State will be transferred to other States, they might become reluctant to engage with the organization, and even refuse to allow it access to the persons an organization seeks to serve. They, too, expect these data to be treated in a Neutral, Impartial and Independent manner.
- Moreover, Humanitarian Organizations that provide aid indiscriminately to persons in need may further engage with non-State armed groups. Sometimes, this may include groups that some States have designated as "terrorist". Without interacting with such groups or individuals, Humanitarian Organizations might not however be in a position to provide essential humanitarian services to affected populations. If those non-State armed groups were to perceive the risk that the Humanitarian Organization might be directly or indirectly compelled to share the contents of their dialogue with governments, this might affect the

42 "The ICRC's privilege of non-disclosure of confidential information", *International Review of the Red Cross*, Vol. 97, No. 897–898 (June 2015), pp. 433–444: https://doi.org/10.1017/S1816383115000533.

43 See on this for example: Council of Delegates of the International Red Cross and Red Crescent Movement, Resolution 12: Safeguarding humanitarian data, 23 June 2022, available at: https://rcrcconference.org/app/uploads/2022/06/CD22-R12-Safeguarding-Humanitarian-Data_23-June-2022_FINAL_EN.pdf; 37th International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy and International Humanitarian Action, 27 October 2015, para. 5 of the Explanatory Statement; 33rd International Conference of the Red Cross and Red Crescent, Resolution 4, December 2019, pp 8 and *op* 8.

organization's perception as neutral. Therefore, those groups might not be willing to interact with Humanitarian Organizations and might potentially prevent the administration of essential humanitarian services to persons under their control.

11.3 MITIGATING THE RISK OF DISCLOSURE OF HUMANITARIAN DATA PROCESSED IN A PUBLIC CLOUD ENVIRONMENT

The preceding sections have shown that it is quintessential for Humanitarian Organizations to make an informed decision about whether to process Humanitarian Data in a public cloud environment, in light of potential disclosure under the legislations and agreements surveyed in Section 11.1 – Mapping legislations allowing governments to require service providers to disclose Humanitarian Data, and the possible impacts such disclosure can have, as set out in Section 11.2 – Impacts of compelled disclosure on Humanitarian Action and persons benefiting from it.

If Humanitarian Organizations choose to process Humanitarian Data in a public cloud environment, they should consider taking the following measures to mitigate the risk of disclosure of such data:

- ensuring the effectiveness of privileges and immunities they may enjoy; and/or
- sensitizing States to the importance of not using or requesting Humanitarian Data for purposes incompatible with their work.

These measures are suggested in addition to the technical, legal and organizational measures explained in Chapter 10: Cloud Services. That said, it is emphasized that Humanitarian Organizations should pay particular attention to encryption. While encryption *per se* cannot mitigate the risk of disclosure of data, it can make it more difficult to use the disclosed data, as such data would not be legible.[44] This is of particular relevance in the context of legal frameworks that do not contain any obligations to furnish decrypted data, such as the CLOUD Act.[45]

11.3.1 ENSURING THE EFFECTIVENESS OF PRIVILEGES AND IMMUNITIES

Some Humanitarian Organizations enjoy privileges and immunities under bilateral or multilateral treaties, or domestic legislation. These are tools that allow them to carry

44 On other technical measures, see European Data Protection Board (EDPB), *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, 18 June 2021, Annex 2: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

45 US Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law around the World*, 18.

out their mandate independently and effectively. Privileges and immunities granted to a Humanitarian Organization remain applicable to data processed in a cloud environment and can therefore in principle serve to prevent the compelled disclosure of data.[46]

Inviolability of archives is particularly pertinent. In the context of the UN, archives have been interpreted to encompass data and infrastructure belonging to, held or used by the organization. Inviolability means, *inter alia*, that a State cannot interfere with those archives, including data, for instance by seizing data.[47] Moreover, immunity from jurisdiction of organizations and their staff can lead to requests for compelled disclosure being declined.

However, the functioning of cloud-specific legislations poses practical obstacles to the effective application of privileges and immunities.

First, some Humanitarian Organizations do not enjoy privileges and immunities universally. For those organizations, whether privileges and immunities can prevent compelled disclosure depends on the availability and scope of the privileges and immunities that the requesting State has granted to the organization. Unless such privileges and immunities are part of customary international law, they only ever bind the State that has granted them to a Humanitarian Organization. They do not establish any obligations on third States. As such, the choice of the service provider and data Processing locations in accordance with the geographical scope of their privileges and immunities are of utmost importance for those organizations.

With a view to the selection of service providers specifically, Humanitarian Organizations might wish to only choose service providers under the jurisdiction of States which have granted privileges and immunities to the organization, and/or that have in place effective blocking statutes. Those can be defined as national legal instruments that prohibit compliance by subjects of national law with requirements

46 European Data Protection Supervisor (EDPS), *Guidelines on the use of cloud computing services by the European institutions and bodies*, 16 March 2018: https://edps.europa.eu/sites/default/files/publication/18-03-16_cloud_computing_guidelines_en.pdf. Equally, the US State Department's position is that documents may retain protection covered by privileges and immunities even if they are in the hands of Third Parties acting as an agent or contractor to the state: Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation, *Implementation of the Virtual Data Embassy Solution: Summary Report of the Research Project on Public Cloud Usage for Government*, n.d.: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmcb.

47 See G. L. Burci, "Inviolability of archives", in *The Conventions on the Privileges and Immunities of the United Nations and Its Specialized Agencies: A Commentary*, Oxford University Press, Oxford, 2016, paras. 8–10.

or prohibitions based on certain foreign laws.[48] One example of such a blocking statute is enshrined in Article 271 of the Swiss Criminal Code, which makes it an offence to "carry out (i) an act reserved to a public authority performed in favour of a foreign State, (ii) on Swiss territory, (iii) without legal entitlement and/or ad hoc authorisation from the Federal Department of Justice and Police and (iv) with a wilful intent to act".[49] As such, depending on the circumstances, the Swiss Blocking Statute may prevent Swiss service providers from assisting foreign authorities in accessing data on Swiss territory without authorization.[50]

In choosing service providers, Humanitarian Organizations should also bear in mind bilateral agreements such as the UK/US agreement, as they could allow States, in which the Humanitarian Organization might not enjoy privileges and immunities, to require disclosure from service providers under the jurisdiction of the other State Party to the agreement.

Moreover, a defining characteristic of Cloud Services is the frequent use of Sub-Processors with access to content and/or meta, traffic or location data. Against this backdrop, Humanitarian Organizations should apply the same considerations as outlined above in selecting or accepting Sub-Processors.

Second, requests under the legislations and case law examined in Section 11.1 – Mapping legislations allowing governments to require service providers to disclose Humanitarian Data enable authorities to require service providers directly to disclose information to authorities, and not the Humanitarian Organization. As such, the Humanitarian Organization might not itself have any standing to rely on their privileges and immunities. This is exacerbated by the fact that some legislations permit authorities to impose a non-disclosure order on the service provider, prohibiting the latter from informing the entity whose information is sought about the disclosure request. As a result, organizations might not even be aware that their data are being sought.

Therefore, if Humanitarian Organizations decide to process Humanitarian Data in a public cloud environment, they should take the following steps to ensure the effectiveness of their privileges and immunities:

48 See the European Commission's definition of blocking statutes: European Commission, "Extraterritoriality (Blocking Statute)", n.d.: https://finance.ec.europa.eu/eu-and-world/open-strategic-autonomy/extraterritoriality-blocking-statute_en.

49 Valentine Bagnoud, Deborah Hondius and Sandrine Giroud, "Swiss Blocking Statute: Update on Do's and Don'ts under the Threat of Criminal Sanctions", LALIVE (blog), 3 December 2019: www.lalive.law/swiss-blocking-statute-update-on-dos-and-donts-under-the-threat-of-criminal-sanctions.

50 On this, see David Rosenthal, "US CLOUD Act: Why It Should Not Prevent Cloud Projects", VISCHER, 2 August 2020: www.vischer.com/en/knowledge/blog/us-cloud-act-why-it-should-not-prevent-cloud-projects-38580.

- Take into account relevant legislations and inter-State agreements, such as the UK/US agreement, in selecting cloud service providers, Sub-Processors and data locations;
- negotiate in their contracts with service providers and other technology providers offering public cloud-based services that, in case of a request, the service providers should at least inform authorities of the fact that the data sought may be subject to privileges and immunities.[51]

For purposes of comprehensiveness, it is noted that Humanitarian Organizations, particularly where they do not enjoy privileges and immunities, may of course also resort to remedies and challenges enshrined in national law. Since the availability and scope of those means vary from State to State, Humanitarian Organizations should make themselves familiar with relevant legislation.

11.3.2 SENSITIZING STATES TO THE IMPORTANCE OF NOT USING OR REQUESTING HUMANITARIAN DATA FOR PURPOSES INCOMPATIBLE WITH THE WORK OF HUMANITARIAN ORGANIZATIONS

To make humanitarian data less vulnerable to disclosure requests in the first place, Humanitarian Organizations may wish to sensitize States to the importance of refraining from using or requesting humanitarian data for purposes incompatible with their work, subject to their mandates and working modalities. To this end, humanitarian organizations could, for example, advocate to:

- exclude Humanitarian Data from the scope of relevant legislations and international agreements; and/or
- obtain otherwise a legally binding commitment from States to refrain from using or requesting Humanitarian Data in a manner incompatible with the mandate and working modalities of the organization.[52]

51 See also Section 10.9 – Privileges and immunities and the cloud.

52 For instance, with a view to the Red Cross and Red Crescent Movement, the 2022 Council of Delegates of the International Red Cross and Red Crescent Movement "emphasizes the fact that the 33rd International Conference urged States and the Movement to cooperate to ensure that humanitarian data are not requested or used for purposes incompatible with the humanitarian nature of the work of the Movement, and in conformity with Article 2 of the Statutes of the Movement, or in a manner that would undermine the trust of the people it serves or the independence, impartiality and neutrality of humanitarian services"; 2022 Council of Delegates, Resolution 12, *supra* fn [45].