CENTER FOR DEMOCRACY & TECHNOLOGY

Memorandum on Human Rights Criteria for Cross-Border Demands

This memorandum supports the human rights criteria that CDT has articulated for cross-border demands for Internet users' communications content. CDT released those criteria on the eve of the European Commission's scheduled release of the E-Evidence initiative. They had been conveyed to the Commission in prior commentary by CDT and other civil society groups. This memorandum articulates legal support for these criteria that is drawn from decisions of the European Court of Human Rights (ECtHR), the Court of Justice of the European Union (CJEU), and from secondary sources as indicated.

Legality

Requests for data should be connected to a crime that the public can find in a statute, and that statute must contain sufficient detail to provide an accused person notice that their actions are unlawful. Requiring that laws be publically available and sufficiently detailed was set forth by the European Court of Human Rights (ECtHR) in *Weber and Saravia v. Germany*,[1] in which the Court was asked to evaluate whether Germany's strategic monitoring surveillance program violated Article 8 (privacy) of the European Convention on Human Rights (ECHR). The Court stated that surveillance must be conducted "in accordance with the law" and explained that this means that "the impugned measure should have some basis in domestic law;" and that "it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him" (para. 84).

This principle was echoed in *Malone v. United Kingdom*, where the ECtHR evaluated whether the interception of postal and telephone communications and the release of information obtained from metering of telephones in the context of a criminal investigation constituted an Article 8 violation. The Court stated that "...the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence" (para. 67).

Judicial Authorization

Requests should receive authorization independent from the executive, preferably from a judicial body, a principle with ample support in human rights case law. In *Zakharov v. Russia*, the ECtHR reviewed a Russian surveillance program for compliance with Article 8 of the ECHR. The Court noted that it "take[s] into account a number of factors in assessing whether... authorisation procedures are capable of ensuring that secret surveillance is not ordered haphazardly, irregularly or without due or proper consideration" (para. 257). The Court emphasized that "the authority competent to authorise the surveillance" must be "sufficiently

[1] This case (as well as others cited throughout this paper) was about intelligence/national security surveillance, which is different from real time surveillance for criminal purposes. Requiring strong human rights protections in the criminal context is even more compelling than in the intelligence/national security context, where the executive's authority is at its zenith.

independent from the executive" (para. 258). The Court observed in reviewing the judiciary's role in the surveillance program that "the authorisation procedures provided for by Russian law are not capable of ensuring that secret surveillance measures are not ordered haphazardly, irregularly or without due and proper consideration" (para. 267).

Further support for judicial authorization is found in *Szabo and Vissy v. Hungary*, an ECtHR case dealing with Hungary's national security surveillance powers. The Court noted that "[T]he rule of law implies, *inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary…. judicial control offering the best guarantees of independence, impartiality and a proper procedure. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge…. Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny….For the Court, supervision by a politically responsible member of the executive, such as the Minister of Justice, does not provide the necessary guarantees" (para. 77).

Probability

Requests should be made with a showing of a high degree of probability of a crime, and that evidence of the crime would be obtained through the surveillance demand. Decisions in the ECtHR have demonstrated that interferences with privacy should be based on sufficient facts that warrant the government action. In *Zakharov*, the ECtHR observed that state surveillance is compliant with ECHR Article 8 when "the authorisation authority's scope of review" is "capable of verifying the *existence of a reasonable suspicion* against the person concerned, in particular, whether there are *factual indications for suspecting* that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security" (para. 260) (emphasis added). Similarly, in *Szabo*, the Court found an Article 8 violation in part because Hungarian law provides "no legal safeguard requiring" one of its law enforcement agencies to establish "a sufficient factual basis for the application of secret intelligence gathering measures…." (para. 71).

In *Iordachi and Others v. Moldova*, a case regarding domestic phone tapping legislation, the ECtHR found an Article 8 violation in part because "the Moldovan legislation does not elaborate on the degree of reasonableness of the suspicion against a person for the purpose of authorising an interception" (para. 51). Similarly in *Dragojevic v. Croatia*, an ECtHR case regarding the surveillance of an alleged drug trafficker, the Court held there was an Article 8 violation in part because the judge executed four surveillance orders and had not been provided or evaluated details of the facts of the case indicating that there was probable cause to believe that the offences had been committed (para. 95).

Particularity
Requests should be specified such that only information relevant to the crime is accessed. Furthermore, requests should, to the best of their ability, identify specific devices, or sources of relevant information. This principle is reflected in *Zhakarov*, in which the ECtHR stated that interception authorization "must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered." This process would be facilitated by the use of specifics like "names, addresses, telephone numbers or other relevant information" (para. 264). Coupled with its language regarding "factual indications" for belief of criminality, and "the existence of reasonable suspicion" (para. 260), the ECtHR opinion reflects a view towards individualizing as much intelligence surveillance as possible . Applying these principles in the criminal context means that targeting should be even more narrowly tailored.

Least Intrusive Means
The interference with the right to privacy that results from intrusive surveillance cannot be justified when less intrusive means are available. In *Dragojevic v. Croatia*, the ECtHR called the government to task because the government's surveillance requests were "essentially based only on a statement referring to the existence of the OSCOC's request for the use of secret surveillance and the statutory phrase that 'the investigation could not be conducted by other means or that it would be extremely difficult'" (para. 95). The Court noted that "[i]t is [] important that the authorising authority – the investigating judge in the instant case – determines whether there is compelling justification for authorising measures of secret surveillance" (para. 93). Authorization was deficient as "[n]o actual details were provided based on the specific facts of the case and particular circumstances indicating a probable cause to believe that the offences had been committed and that the investigation could not be conducted by other, less intrusive, means" (para. 95).

The Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism was even more explicit. Special Rapporteur Ben Emmerson observed that "[i]t is incumbent upon States to demonstrate that any interference with the right to privacy under article 17 of the [ICCPR] is a necessary means to achieving a legitimate aim. This requires that there must be a rational connection between the means employed and the aim sought to be achieved. It also requires that the measure chosen be "the least intrusive instrument among those which might achieve the desired result" (para. 51). While his analysis was in reference to mass surveillance, the same principle should apply to more circumscribed criminal law enforcement surveillance regimes.

Seriousness
These surveillance requests should only extend to matters in which the underlying crime being investigated is serious, an indication of which is if a significant period of incarceration may be imposed as a result of conviction. The Court of Justice of the European Union (CJEU) touched on this in *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home*

Department v. Tom Watson, cases which considered Swedish and U.K. laws mandating that communications service providers retain customer communications data in bulk for the purpose of preventing and detecting serious crime. The CJEU ultimately found the laws which authorized indiscriminate collection violated Article 8, and noted that "only the objective of fighting serious crime is capable of justifying such a measure … in particular organized crime and terrorism ...." (para. 115).

Other court cases have highlighted the need for surveillance to be targeted at serious crimes. In *Zakharov*, the Court observed with concern that "Russian law allows secret interception of communications in respect of a very wide range of criminal offences, including for example, as pointed out by the applicant, pickpocketing" (para. 244). Furthermore, in *Iordachi and Others*, the Court stated that it "considers it necessary to stress that telephone tapping is a very serious interference with a person's rights and that only very serious reasons based on a reasonable suspicion that the person is involved in serious criminal activity should be taken as a basis for authorising it" (para. 51).

Notice

Users should be notified that their information has been sought or obtained. This notice may be delayed in limited circumstances in order to protect the integrity of the investigation. In *Tele2 Sverige AB* and *Watson* the Court stressed that "the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities" (para. 121). Likewise, in *Zakharov* the ECtHR emphasized that "[a]s soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned" (para. 287) and that "[t]he effectiveness of the remedies is undermined by the absence of notification at any point of interceptions, or adequate access to documents relating to interceptions" (para. 302).

Minimization

Information collected through cross-border data requests should be subjected to minimization procedures such that only information necessary to the investigation is retained, and excess information that is collected should be destroyed or returned. This principle is found enshrined in *S. and Marper v. the United Kingdom*, an ECtHR case which held that holding DNA samples of individuals arrested but who are later acquitted or have the charges against them dropped violated their right to privacy. The court explained, "The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article...The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved

in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored...[It] must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse...." (para. 103).

The ECtHR in *Kennedy v. United Kingdom* found that the surveillance practice the court was reviewing abided by Article 8 in part because national legislation required that the "intercept material and any related communications data, as well as any copies made of the material or data, must be destroyed as soon as there are no longer any grounds for retaining them as necessary" and because that legislation also required that "intercept material must be reviewed at appropriate intervals to confirm that the justification for its retention remains valid" (para. 164). Similarly in *Weber*, the court noted that having policies in place like "the destruction of personal data as soon as they were no longer needed to achieve their statutory purpose, and for the verification at regular, fairly short intervals of whether the conditions for such destruction were met" were useful "safeguards against abuse of the State's powers of surveillance" (para. 132).

Transparency

This system must include the publication of the numbers of data demands made and granted, and types of offenses for which the data was requested must be specified. Although this is not explicitly mandated by any ruling, it is implied in how the ECtHR has evaluated surveillance systems. Indeed, in Weber the ECtHR observed that, "In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse" (para. 106). Likewise, the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights observed in their report on Freedom of Expression and the Internet that, "States should disclose general information on the number of requests for interception and surveillance that have been approved and rejected, and should include as much information as possible, such as—for example—a breakdown of requests by service provider, type of investigation, time period covered by the investigations, etc" (para. 168).

Redress

Cross-border data demand regimes must provide individuals the ability to seek redress. In reaching the conclusion that Hungary had violated Article 8, the ECtHR in Szabo pointed to the inability of individuals subject to the surveillance regime to seek redress, "In total sum, the Court is not convinced that the Hungarian legislation on "section 7/E (3) surveillance" provides safeguards sufficiently precise, effective and comprehensive on the ordering, execution and potential redressing of such measures" (para. 89). Further, the Court stated that it was "not persuaded that this scrutiny is able to provide redress to any individual grievances caused by secret surveillance" (para. 82).

CENTER FOR DEMOCRACY & TECHNOLOGY

Conclusion

This memorandum outlines legal support for ten human rights criteria for cross-border demands for internet users' communications. Those criteria should be applied to the European Commission's E-Evidence initiative as well as to other efforts to facilitate cross-border data demands for law enforcement purposes. For further information, please contact Greg Nojeim, Director, CDT Freedom, Security and Technology Project (gnojeim@cdt.org) or Mana Azarmi, CDT Legal Fellow (mazarmi@cdt.org).