September 20, 2022

To:

The Information and Communication Technology Division, Bangladesh:

(1) Mr. Md Shakhawat Hossain
Deputy Secretary, Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology
Government of People's Republic of Bangladesh
E-14/X, BCC Bhaban, Agargaon
Dhaka 1207, Bangladesh
E-mail: shakhawat.hossain@ictd.gov.bd

(2) Ms. Sadia Afroz
Senior Assistant Secretary, Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology
Government of People's Republic of Bangladesh
E-14/X, BCC Bhaban, Agargaon
Dhaka 1207, Bangladesh
E-mail: sadia.afroz@ictd.gov.bd

Access Now's Additional Submission to the Information and Communication Technology Division, Bangladesh, on the Draft Data Protection Act, 2022

We thank the Information and Communication Technology Division ("**ICTD**") for the opportunity to submit additional comments on the Draft Data Protection Act, 2022. Our submission on the previous draft is attached as Annexure I.

About Access Now

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence in 13 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights.

Access Now also engages with its global community of nearly half a million users from over 185 countries, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We coordinate as part of CiviCERT (Computer Incident Response Center for Civil Society) a Trusted Introducer accredited CERT, and are a member of the global Forum of Incident Response and Security Teams (FiRST). We have special consultative status at the United Nations.[1]

Access Now has consistently engaged with multiple stakeholders around the world, including governments and regulatory authorities, on the creation of a robust data protection regime.[2] We write to you to provide our comments based on our expertise working on digital rights in various regions across the world, including the Asia Pacific.

Additional Submissions on the Draft Data Protection Act, 2022

In light of the rampant increase in data collection, storage, usage and disclosure practices, around the globe, as well as in Bangladesh, there is an urgent need to implement a robust legislative framework in the country. Such a framework must enable transparency and accountability from the private sector as well as the government and law enforcement agencies; protect and strengthen people's right to privacy, and autonomy over the lifecycle of their information. The development of the Draft Data Protection Act, 2022, ("**Draft Act**"), with inputs from all stakeholders, is an important step towards implementing effective checks, balances and safeguards that uphold fundamental rights.

---

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.
[2] See for example, Access Now, *Protecting Our Data,* https://www.accessnow.org/issue/data-protection/page/2/ ; Access Now, *Three Years Under the GDPR: An Implementation Progress Report*, https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf ; Access Now, *India's data protection bill: Further work needed in order to ensure true privacy for the next billion users*, https://www.accessnow.org/cms/assets/uploads/2020/02/Access-Now-Analysis-Indias-Personal-Data-Protection-Bill-2019.pdf ; Access Now, *The Right to Privacy in Indonesia*, https://www.accessnow.org/cms/assets/uploads/2022/04/ELSAM-and-Access-Now-UPR-Joint-Submission-on-the-Right-to-Privacy-in-Indonesia.pdf.

The ICTD's initiative to formulate a data protection framework is very welcome, and we commend the ICTD for incorporating revisions and making revised iterations of the Draft Act available for public comment.

We humbly submit that the Draft Act would need to be modified further to be made into a rights-respecting, effective law, and we request the ICTD to secure additional stakeholder input, including from civil society, privacy and cybersecurity experts, small and medium enterprises, as well as the public at large. To this end, we submit our feedback on the most recent draft and welcome the opportunity provided by the ICTD to do so.

In addition to the comments in our present and previous submissions, we also submit as attachments to this document (a) a copy of our guide for lawmakers titled "Creating a Data Protection Framework: A Do's and Don't's Guide for Lawmakers" as Annexure II[3]; and (b) a copy of the "Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance" as Annexure III.[4] We request that these documents may please be perused as forming part of our substantive feedback on the creation of a rights-respecting data protection framework.

Limit data retention mandates under the Draft Act

Section 25 of the Draft Act prescribes that data processed for a purpose shall not be retained for a period longer than the period prescribed by the rules for that purpose. Further, Section 27 states that subject to Section 25, the controller must retain all records regarding the data processed. These provisions appear contradictory, they lack meaningful limitations and could result in extensive and unreasonable retention of data.

There are primarily three issues with the data retention mandates in these provisions. First, in the absence of rules, there is no clarity, and therefore scope for exploitation, in respect of the timeline and methods for data retention. Second, in any case, limitations on data retention have a direct impact on people's rights, and must therefore be embedded within legislation passed with parliamentary and public scrutiny, as opposed to being left to the discretion of the executive and its rule-making powers. Any provision pertaining to the retention of data, must provide for adherence with principles of data minimisation[5], purpose limitation,

---

[3] Access Now, *Creating a Data Protection Framework: A Do's and Don't's Guide for Lawmakers*, https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf

[4] Access Now, *Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance*, https://www.accessnow.org/cms/assets/uploads/archive/docs/Implementation_guide_-_July_10_print.pdf

[5] Access Now, *Data Minimisation, Key to Protecting Privacy and Reducing Harm*, https://www.accessnow.org/cms/assets/uploads/2021/05/Data-Minimization-Report.pdf ; Access Now,

necessity and proportionality[6], in order to safeguard people's rights and prevent selective interpretation and a "collect it all" approach. And third, in the absence of such built-in limitations and safeguards, the mandate in Section 27 to to retain all records regarding the data processed is overbroad and disproportionate, and could lead to undue and extensive retention of data, including people's personal data and metadata that could be used to infer more data.

Access Now recommends that Sections 25, 27 and any other provision on retention of data, must categorically provide for adherence with principles of data minimisation, purpose limitation, necessity and proportionality. Such limitations must be incorporated within the legislative framework, and not be left to the discretion of the executive and its rule-making power.

Wide scope of exemptions and overbroad discretionary powers for the government

We reiterate our comments on this issue in the previous submission as the underlying provisions remain the same.

No matter how many provisions a data protection legislation purports to carry to preserve people's rights and data, they are meaningless if accompanied by wide and overbroad exceptions that can be misused to circumvent the protective mechanisms.

The current draft of the Act contains too wide a scope for exemptions to meaningfully protect data and guard against misuse and abuse of powers by both the private and the public sector. For example, Section 33 allows for exemptions to be granted from the application of any provision under the Draft Act for a broad range of purposes. The scope of exemptions, the circumstances in which – and the authority by whom – they may be applied is not clearly defined; the provision does not carry any meaningful limitations, and fails to lay down a procedure to ensure transparency and accountability and adherence with principles of necessity and proportionality.[7]

Further, under Section 34, the government has unfettered discretionary powers to grant exemptions for any Controller from application of any provision in the Draft Act. The government is also empowered to impose the necessary conditions relating to the exemptions. This is neither necessary nor proportionate. Such a broad exemption also limits

---

Why data minimisation matters for safe data transfers and more, https://www.accessnow.org/why-data-minimisation-matters-for-data-transfers/

[6] Coalition of international organisations and experts, *Necessary and Proportionate*, https://necessaryandproportionate.org/principles/

[7] Same as footnote 6.

independent oversight and control over the way a controller may use personal data. A rights-respecting data protection regime cannot be achieved without limitations on the government's powers and safeguards against arbitrary decisions and misuse of powers by the government.

Access now recommends that the Draft Act be amended to strictly restrict the scope for exemptions through clear and narrow definitions; impose meaningful limitations on the government's powers; and incorporate safeguards aligned with the principles of necessity and proportionality, to protect people's data and privacy. For clarity and to provide legal certainty, the government shall not have discretionary powers to limit the application of rules to be laid down in the Act to any controller.

Independence of the Data Protection Office

The establishment of a completely independent supervisory and regulatory authority is an essential element of an effective data protection framework. A data protection law would be meaningless without an independent authority having the powers and resources to monitor implementation, conduct investigations, address complaints, provide remedies through a concrete enforcement mechanism, enable transparency and accountability, and impose sanctions and penalties.

We appreciate that provisions have been amended to bring the proposed Data Protection Office (DPO) outside the fold of the Digital Security Agency (DSA), as had also been recommended in our previous submission. The DSA must have absolutely no direct or indirect influence over the DPO. However, despite this first improvement, the DPO continues to lack independence on account of extensive government control. We humbly submit that significant amendments are necessary to ensure complete independence of the DPO and eliminate any scope for executive influence.

Under the current draft, the government retains the ability to control the functioning of the DPO. For instance, Section 36 of the Draft Act empowers the government to appoint the Director General as well as the other Directors of the DPO, and requires the DPO to comply with policy guidelines adopted by the government regarding its functioning and duties. Moreover, Section 40 mandates prior government approval to formulate Standard Operating Rules relating to the collection, processing, storing or retention, or use of data, and a host of other issues covering nearly the entire information lifecycle and directly impacting people's rights.

This contravenes a central tenet of a meaningful data protection framework, which is the requirement of absolute independence of the regulatory authority from any government influence or control, whether direct or indirect, including in the role of the chairperson/chief and members, the process of appointment, policymaking, formulation of standard operating procedures and overall functioning. The Government and its agencies are typically among the most prominent data collectors and processors of people's personal information. An effective data protection framework must therefore ensure that the regulatory authority is in a position to deliver impartial and just decisions, including against the government if necessary.

Access Now recommends that the overall scheme of the Draft Act be amended to ensure that the Data Protection Office is completely independent from the government and its agencies, including in its composition, appointments, formulation of policies and guidelines, procedures and functioning. The Data Protection Office may cooperate and coordinate action with other independent regulatory authorities once established but their powers, functions, and responsibilities should not be conflated.

Appeal and judicial remedy

In addition to the government being granted extensive discretionary powers and control over the DPO, it has also been made the appellate authority against decisions of the Director General of the DPO under Section 59. Therefore, at both these levels, affected individuals would not have any avenue for remedy and redressal that is completely independent of the government, even if, as may often be the case, the complaint is against a controller linked to the government.

The Draft Act currently lacks a robust mechanism for effective remedy that confers actionable rights upon individuals and entities with respect to their data, an independent authority to investigate and enforce such rights. In addition to an independent regulatory authority with binding decision-making powers, judicial oversight and accessible remedy constitute crucial components of a meaningful data protection regime. The appellate authority ought to be an independent adjudicatory body, and not the government, with clear avenues to avail of judicial remedy.

Access Now recommends that the Draft Act be amended to establish a direct right of action, supported by a clearly set out mechanism for complaints and redressal, with accessible judicial remedy. Aggrieved persons and entities must have the right to approach an independent adjudicatory authority with complaints and appeals to seek remedy, such power of adjudication must not be vested in the government.

Data localisation

Section 44 of the Draft Act stipulates that sensitive data, user generated data and classified data shall be stored only in Bangladesh. We appreciate that, in this context, the definition of "sensitive data" has been modified to eliminate "religious or political belief or opinion", which partially addresses the concern noted in our previous submission regarding its potential to include any exercise of free expression on social media. However, as noted below, further amendments are necessary. We reiterate our comments in our previous submission as the underlying provisions remain the same.

Classified data could be any data that may be classified as such by the government from time to time. No guidance has been provided regarding the criteria to be met and procedures to be followed for the classification of "classified data". The decision has been left entirely up to the discretion of the government. Such proposals conferring blanket powers on the government impacting privacy and cross-border flow of data, go against the spirit and objective of comprehensive data protection and privacy legislation.

Further, "user generated data" has not been defined in the Draft Act. This could potentially serve as a catch-all category that includes several types of data and would have a detrimental effect on the free flow of data across borders. Further, this category could include any exercise of free expression on social media, including to target dissent and unpopular opinions – particularly because the definition of sensitive data in Section 2(21) includes "religious or political belief or opinion" – which could then be stifled, subjected to localisation requirements, and prevented from being shared freely.

Stringent data localisation provisions such as those in the Draft Act also contribute towards exacerbating the vulnerability of people's privacy and free speech as they amplify the government's access to and control over data. While it is important to safeguard the rights of users and protect sensitive personal data, the measures proposed in the Draft Act would do the opposite. The absence of surveillance reform, procedural checks and substantive oversight of data access and interception powers of government authorities puts data mandated to be stored in the country at risk as they could be accessed and misused by public authorities from Bangladesh but also by third countries.

Existing laws and regulatory frameworks in Bangladesh allow for any data stored in Bangladesh to be subjected to surveillance, monitoring and interception efforts, as well as data disclosure or removal requests, by government and intelligence agencies, who could be exempt from the Draft Act.

Insufficient safeguards to protect people's data and undue restrictions such as mandated data localisation may also undermine Bangladesh's trade prospects with other territories, such as the European Union, the United Kingdom, and the United States, which place restrictions on transfer of personal data unless the country provides an adequate level of protection for the rights and freedoms of users in relation to the processing of personal data. Consequently, people in Bangladesh may be deprived of access to internationally available services, thereby placing them at a disadvantage and negatively impacting rights, accessibility and growth.

Access Now recommends that data localisation requirements be eliminated from the Draft Act; provisions be incorporated in the Draft Act to propel surveillance reform with the aim of protecting human rights; and robust substantive and procedural protections for privacy be implemented, also to enable cross-border data flows.

Notice of data breach to affected individuals

Section 28 of the Draft Act, requires the controller to inform the Director General in the event of a data breach. However, there is no strict notice requirement to data subjects and affected individuals under the Draft Act.

Notice to users should be a strict requirement for data breach. Such notice should be timely, easy to understand, and comprehensive, and options for remedy should be clearly explained and made accessible. In the absence of such a requirement, the Draft Act falls short of empowering users to take control of their information. Data controllers in the private and the public sector have an economic and reputational interest in downplaying the risks associated with a breach and not notifying users, which could result in unaddressed data protection violations. Additionally, unclear provisions that require data controllers to first notify a public sector agency on a data breach, the Director General in this case, but do not make it clear that they should also notify impacted individuals have the effect of paralysing these controllers, as they wait until they are explicitly told that they can notify users, or create room for shifting of blame. We encourage lawmakers to avoid those shortcomings and develop unambiguous data breach prevention and notification mechanisms.

Access Now recommends that the Draft Act be amended to mandate that users and affected individuals be notified in a timely and comprehensive manner, with clear articulation of available remedies, in the event of a data breach. We recommend breach to be notified to affected individuals within 72 hours of discovery.

Conclusion

Thank you for the opportunity to participate in this consultation. We remain available for any clarification or queries in relation to this feedback, and hope to be of further assistance in this important process.

Yours sincerely,

Namrata Maheshwari
Asia Pacific Policy Counsel
namrata@accessnow.org r

Raman Jit Singh Chima
Senior International Counsel and Asia Pacific Policy Director
raman@accessnow.org

Access Now | https://www.accessnow.org

[*This submission was prepared with the assistance of Estelle Massé, Global Data Protection Lead at Access Now*]

Annexure I

April 27, 2022

To:

The Information and Communication Technology Division, Bangladesh:

(1) Dr. Sirat Mahmuda
Deputy Secretary, Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology
Government of People's Republic of Bangladesh
E-14/X, BCC Bhaban, Agargaon
Dhaka 1207, Bangladesh
E-mail: sirat.mahmuda@ictd.gov.bd

(2) Mr. Ranajit Kumar
Additional Secretary (Law & Policy Wing)
Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology
Government of People's Republic of Bangladesh
E-14/X, BCC Bhaban, Agargaon
Dhaka 1207, Bangladesh
E-mail: ranajit.kumar@ictd.gov.bd

Submission to the Information and Communication Technology Division, Bangladesh, on the Draft Data Protection Act, 2022

We thank the Information and Communication Technology Division for the opportunity to submit comments on the Draft Data Protection Act, 2022.

About Access Now

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence in 13 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights.

Access Now also engages with its global community of nearly half a million users from over 185 countries, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We coordinate as part of CiviCERT (Computer Incident Response Center for Civil Society) a Trusted Introducer accredited CERT, and are a member of the global Forum of Incident Response and Security Teams (FiRST). We have special consultative status at the United Nations.[1]

Access Now has consistently engaged with multiple stakeholders around the world, including governments and regulatory authorities, on the creation of a robust data protection regime.[2] We write to you to provide our comments based on our expertise working on digital rights in various regions across the world, including the Asia Pacific.

Submissions on the Draft Data Protection Act, 2022

The Draft Data Protection Act, 2022, ("**Draft Act**") is an important step towards ensuring that people's right to privacy in Bangladesh is protected, and people's autonomy over their information is prioritised in the digital age. The multiplicity and ubiquity of digital services and internet intermediaries, and unchecked practices of data collection, usage and sharing, combined with lack of transparency and effective legal safeguards to protect people's rights, have made it imperative for a robust framework safeguarding people's rights and freedoms to be implemented. The initiative to formulate a data protection framework is very welcome;

---

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.
[2] See for example, Access Now, *Protecting Our Data,* https://www.accessnow.org/issue/data-protection/page/2/ ; Access Now, *Three Years Under the GDPR: An Implementation Progress Report*, https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf ; Access Now, *India's data protection bill: Further work needed in order to ensure true privacy for the next billion users*, https://www.accessnow.org/cms/assets/uploads/2020/02/Access-Now-Analysis-Indias-Personal-Data-Protection-Bill-2019.pdf ; Access Now, *The Right to Privacy in Indonesia*, https://www.accessnow.org/cms/assets/uploads/2022/04/ELSAM-and-Access-Now-UPR-Joint-Submission-on-the-Right-to-Privacy-in-Indonesia.pdf.

however, we humbly submit that the Draft Act would need to be modified significantly to be made into a rights-respecting, effective law, and we request the Information and Communication Technology Division ("**ICTD**") to secure more stakeholder input for its drafting and implementation. To this end, we submit our initial feedback on the Draft Act and welcome the opportunity provided by the ICTD to do so.

In addition to the comments in this submission, we also submit as attachments to this document (a) a copy of our guide for lawmakers titled "Creating a Data Protection Framework: A Do's and Don't's Guide for Lawmakers" as Annexure I[3]; and (b) a copy of the "Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance" as Annexure II.[4] We request that these documents may please be perused as forming part of our substantive feedback on the creation of a rights-respecting data protection framework.

Extension of timeline to provide comments

The Draft Act aims to fill a crucial legislative vacuum that will have a direct impact on Constitutional and human rights. Sustained and in-depth feedback from all stakeholders is integral to the development of such legislation. We appreciate the ICTD's initiative to invite public comments on the draft. However, we respectfully submit that the present period for public consultation of less than five weeks, is inadequate and will not enable wider participation which is essential to a democratic process.

In addition to the importance of engaging with people, communities and organisations in Bangladesh, given the cross-border implications of a data protection regime, feedback from the international community, including experts on the subject, would also contribute towards the development of an effective framework that builds on the experiences of other regions. Therefore, we request that the consultation period be extended to enable sustained engagement and contributions from the full range of government and non-government stakeholders within Bangladesh and globally, including civil society organisations, security experts, private sector, industry associations.

---

[3] Access Now, *Creating a Data Protection Framework: A Do's and Don't's Guide for Lawmakers*, https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf

[4] Access Now, *Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance*, https://www.accessnow.org/cms/assets/uploads/archive/docs/Implementation_guide_-_July_10_print.pdf

Independence of the Data Protection Office

A data protection framework is incomplete and ineffective without a robust enforcement mechanism which includes the creation of an absolutely independent supervisory authority. A data protection law would be meaningless without an independent authority having the powers and resources to monitor implementation, conduct investigations, address complaints, provide remedies through a concrete enforcement mechanism, enable transparency and accountability, and impose sanctions and penalties.

The proposed regulatory authority, i.e. the Data Protection Office (DPO), as currently contemplated in the Draft Act, completely lacks independence from the government. For instance, Section 35 of the Draft Act states that the DPO shall be under the administration and control of the Digital Security Agency (DSA) as established under Digital Security Act, 2018; and the Director General of the DSA shall be the chief of the DPO. Further, the government is empowered to appoint officers and employees as necessary for the purpose of properly conducting the functions of the DPO.

This contravenes a central tenet of a meaningful data protection framework, which is the requirement of absolute independence of the regulatory authority from any government influence or control, whether direct or indirect, including in the role of the chairperson/chief and members, the process of appointment, policymaking, and overall functioning. The Government and its agencies are typically among the most prominent data collectors and processors of people's personal information. An effective data protection framework must therefore ensure that the regulatory authority is in a position to deliver impartial and just decisions, including against the government if necessary.

Separately, while the influence of any government agency must be avoided, we specifically caution against the involvement of the DSA in the creation and implementation of the Draft Act. The Draft Act will determine the course of people's right to privacy in Bangladesh, and given the surge in invocation of provisions in the Digital Security Act to quell freedom of expression[5], people will have greater confidence in the process if the DSA is not entrusted with any responsibility pertaining to the Draft Act.

Access Now recommends that the overall scheme of the Draft Act be amended to ensure that

[5] Article 19, *Bangladesh: Alarming crackdown on freedom of expression during coronavirus pandemic*, https://www.article19.org/resources/bangladesh-alarming-crackdown-on-freedom-of-expression-during-coronavirus-pandemic/

the Data Protection Office is completely independent from the government and its agencies, including in its composition, appointments, procedures and functioning. The Data Protection Office may cooperate and coordinate action with other independent regulatory authorities once established but their powers, functions, and responsibilities should not be conflated.

Wide scope of exemptions and overbroad discretionary powers for the government

No matter how many provisions a data protection legislation purports to carry to preserve people's rights and data, they are meaningless if accompanied by wide and overbroad exceptions that can be misused to circumvent the protective mechanisms.

The current draft of the Act contains too wide a scope for exemptions to meaningfully protect data and guard against misuse and abuse of powers by both the private and the public sector. For example, Section 33 allows for exemptions to be granted from the application of any provision under the Draft Act for a broad range of purposes. The scope of exemptions, the circumstances in which – and the authority by whom – they may be applied is not clearly defined; the provision does not carry any meaningful limitations, and fails to lay down a procedure to ensure transparency and accountability and adherence with principles of necessity and proportionality.[6]

Further, under Section 34, the government has unfettered discretionary powers to grant exemptions for any Controller from application of any provision in the Draft Act. The government is also empowered to impose the necessary conditions relating to the exemptions. This is neither necessary nor proportionate. A rights-respecting data protection regime cannot be achieved without limitations on the government's powers and safeguards against arbitrary decisions and misuse of powers by the government.

Access now recommends that the Draft Act be amended to strictly restrict the scope for exemptions through clear and narrow definitions; impose meaningful limitations on the government's powers; and incorporate safeguards aligned with the principles of necessity and proportionality, to protect people's data and privacy.

Data localisation

Section 42 of the Draft Act stipulates that sensitive data, user generated data and classified

[6] Coalition of international organisations and experts, *Necessary and Proportionate*, https://necessaryandproportionate.org/principles/

data shall be stored only in Bangladesh. Sensitive data has been defined in Section 2(21) and includes “religious or political belief or opinion”. This could include any exercise of free expression on social media as well.

Classified data would be any data that may be classified as such by the government from time to time. No guidance has been provided regarding the criteria to be met and procedures to be followed for the classification of “classified data”. The decision has been left entirely up to the discretion of the government. Such proposals conferring blanket powers on the government impacting privacy and cross-border flow of data, go against the spirit and objective of comprehensive data protection and privacy legislation.

Further, “user generated data” has not been defined in the Draft Act. This could potentially serve as a catch-all category that includes several types of data and would have a detrimental effect on the free flow of data across borders. Further, this category could include any exercise of free expression on social media, including to target dissent and unpopular opinions – particularly because the definition of sensitive data in Section 2(21) includes “religious or political belief or opinion” – which could then be stifled, subjected to localisation requirements, and prevented from being shared freely.

Stringent data localisation provisions such as those in the Draft Act also contribute towards exacerbating the vulnerability of people’s privacy and free speech as they amplify the government’s access to and control over data. While it is important to safeguard the rights of users and protect sensitive personal data, the absence of surveillance reform, procedural checks and substantive oversight of data access and interception powers of government authorities puts data mandated to be stored in the country at risk as they could be accessed and misused by public authorities from Bangladesh but also by third countries.

Existing laws and regulatory frameworks in Bangladesh allow for any data stored in Bangladesh to be subjected to surveillance, monitoring and interception efforts, as well as data disclosure or removal requests, by government and intelligence agencies, who could be exempt from the Draft Act.

Insufficient safeguards to protect people’s data may also undermine Bangladesh’s trade prospects with other territories, such as the European Union, the United Kingdom, and the United States, which place restrictions on transfer of personal data unless the country provides an adequate level of protection for the rights and freedoms of users in relation to the processing of personal data. Consequently, people in Bangladesh may be deprived of access

to internationally available services, thereby placing them at a disadvantage and negatively impacting rights, accessibility and growth.

Access Now recommends that data localisation requirements be eliminated from the Draft Act; provisions be incorporated in the Draft Act to propel surveillance reform with the aim of protecting human rights; and robust substantive and procedural protections for privacy be implemented, also to enable cross-border data flows.

Principles of data protection, and mechanism for redress and judicial remedy

Principles of data protection

We commend the inclusion in the Draft Act of principles that must be observed with respect to the collection,use, retention and other processing of data.

In addition to the principles set out in Section 5 of the Draft Act, principles of necessity and proportionality should be included. These principles have been widely recognised across the globe as essential elements of a human rights framework.

Additionally, we urge that the data minimisation and purpose limitation principles also be included. Personal data collected and used should be limited to what is adequate, relevant, and not excessive in relation to a specific and defined purpose.[7]

Access Now recommends that the Draft Act be amended to include the principles of necessity and proportionality, which must inform any type of collection, processing, use or retention of data.

Mechanism for redress and judicial remedy

The Draft Act currently lacks a robust mechanism that confers actionable rights upon individuals and entities with respect to their data, an independent authority to investigate and enforce such rights.

In addition to an independent regulatory authority with binding decision-making powers, judicial oversight and accessible remedy constitute crucial components of a meaningful data

[7] Access Now, *Data Minimisation, Key to Protecting Privacy and Reducing Harm*, https://www.accessnow.org/cms/assets/uploads/2021/05/Data-Minimization-Report.pdf

protection regime.

The enforcement of rights at present, under Section 20, is subject to rules that may be prescribed by the government. The legislation itself does not create a direct right of action, supported by a clearly set out mechanism for complaints and redressal, with accessible judicial remedy.

Further, the redressal mechanism established under Chapter XII, places the power to make decisions on complaints in the hands of the government, and not an independent adjudicatory authority. Section 46 states that any person who believes that her rights have been violated may file a complaint with the Director General of the Digital Security Agency under the Government. Thereafter, Section 56 provides that any person aggrieved by a decision or order under this chapter may appeal to the Government.

Access Now recommends that the Draft Act be amended to establish a direct right of action, supported by a clearly set out mechanism for complaints and redressal, with accessible judicial remedy. Aggrieved persons and entities must have the right to approach an independent adjudicatory authority with complaints and appeals to seek remedy, such power of adjudication must not be vested in the government.

Broad rule-making powers

The Draft Act presently provides for excessive rule-making powers accorded to the government authorities. Sections 18, 19, 20, 22, 24, 29, 53, and 69, are among the many provisions that confer rule-making powers upon the government.

While provisions for rulemaking may be required in some circumstances, there is a need to ensure that such provisions are limited to prevent misuse. As much as possible should be specified in the legislation itself, particularly with respect to scope and procedures for access, storage and disclosure of data, and the mechanism for affected parties to enforce their rights and seek remedy and redress.

For instance, Section 20 on the conditions for exercise of rights stipulates that the exercise of any rights by the data subject, steps to be undertaken by the Controller in relation to the subject's request, and refusal of request by the Controller, and any other related matters, shall be prescribed by rules. The procedure for enforcement of rights is pivotal to a rights-based data protection regime and must be prescribed in legislation which is formulated after taking

into account inputs of all stakeholders through in-depth consultation and passed by the parliament, and not by executive rule-making powers which are far more centralised and prone to misuse.

Access Now recommends that the government's rule-making powers under the Draft Act be restricted, and as much as is possible be prescribed in legislation formulated through a democratic process of participation and parliamentary procedures, particularly provisions with respect to scope and procedures for access, storage and disclosure of data, and the mechanism for affected parties to enforce their rights and seek remedy and redress.

Ambiguity in language across the Draft Act

Ambiguous language in legislation can result in dilution of well-intentioned provisions aimed at protecting data and privacy, and an increase in scope for misuse. Clear language and predictability on the scope of application of the Draft Act would be beneficial for all stakeholders including individuals, businesses and government agencies.

For instance, Section 57 of the Draft Act states that in case of a complaint brought to the Director General for violation of any provision of the Act, if it appears to the Director General that the payment of administrative fine is not sufficient to remedy the violation, the Director General may consider the matter of the complaint as an "offence" under this Act, and return the complaint to the concerned person, with specific instructions on what needs to be done, in order to obtain appropriate legal redress. The term "offence" has not been clearly defined anywhere in the Draft Act. This uncertainty regarding what may constitute an offence, and the unfettered discretion granted to the Director General as a result, would result in inconsistent application of the principles of data protection and confusion among affected parties regarding the permissibility of various acts pertaining to data collection, usage, retention and disclosure.

As another example, Section 9 provides that any collector, processor or controller shall not collect, process or retain data in a manner where there is any possibility of infringement of the right to privacy of the data subject. The intention of prioritising the right to privacy is commendable and we support the view that the right to privacy must underpin all data oriented activities. However, in order to achieve this objective in practice, it is necessary to clarify the factors that must be considered and procedures that must be followed while assessing the "possibility of infringement of the right to privacy". This would help enable foreseeability and meaningfully protect privacy.

Access Now recommends that throughout the Draft Act, ambiguous and unclear language which may result in confusion, misuse or inaction be replaced by clear definitions of scope, application and procedure, to enable legal certainty and foreseeability and meaningfully protect privacy.

Notice and reporting requirements

The Draft Act, under Section 28 of the Draft Act, requires the controller to inform the Director General in the event of a data breach. However, there is no strict notice requirement to data subjects and affected individuals under the Draft Act. In this context, Section 36 merely states that the DPO has the power to direct the controller to communicate with the data subject in case of a data breach.

Notice to users should be a strict requirement for any data breach. Such notice should be timely, easy to understand, and comprehensive, and options for remedy should be clearly indicated and accessible. By leaving too much to the discretion of the DPO and controllers, the provisions in the Draft Act fall short of empowering users to take control of their information. Data controllers in the private and the public sector have an obvious economic and reputational interest in downplaying the risks associated with a breach and not notifying users, which could result in unaddressed data protection violations. Additionally, unclear provisions that require data controllers to first notify a public sector agency on a data breach but do not make it clear that they should also notify impacted individuals has the effect of paralysing these controllers, as they wait until they are explicitly told that they can do user notification. We encourage lawmakers around the world to avoid those shortcomings and develop unambiguous data breach prevention and notification mechanisms.

Access Now recommends that the DPA be amended to mandate that users and affected individuals be notified in a timely and comprehensive manner, with clear articulation of available remedies, in the event of a data breach. We recommend breach to be notified to affected individuals within 72 hours of discovery.

Conclusion

Thank you for the opportunity to participate in this consultation. We remain available for any clarification or queries in relation to this feedback, and hope to be of further assistance in this important process.

Yours sincerely,

Namrata Maheshwari
Asia Pacific Policy Counsel
namrata@accessnow.org r

Raman Jit Singh Chima
Senior International Counsel and Asia Pacific Policy Director
raman@accessnow.org

Access Now | https://www.accessnow.org

[*This submission was prepared with the assistance of Estelle Massé, Global Data Protection Lead at Access Now*]

Annexure II

CREATING A DATA PROTECTION FRAMEWORK: A DO'S AND DON'TS GUIDE FOR LAWMAKERS

LESSONS FROM THE EU GENERAL DATA PROTECTION REGULATION

accessnow.org

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

November 2018

This paper is an Access Now publication.

For more information, please visit: **https://www.accessnow.org,** or contact: **Estelle Masse** | Senior Policy Analyst | **estelle@accesnow.org**

TABLE OF CONTENTS

INTRODUCTION

Access Now presents *Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers - Lessons from the EU General Data Protection Regulation to contribute to the global discourse on data protection*. The paper particularly reflects on the European Union's approach to the debate and the level of protection for personal data around the world.

The General Data Protection Regulation (GDPR) of the European Union is a positive framework for users' protection and will help users take back the control of their personal information. While the law is currently being implemented, it is already inspiring governments around the world to upgrade or develop data protection legislation, which brings massive opportunities. There are important lessons to be learned from the negotiations of the GDPR, many positive and some negative.[1] From our experience, we have created a list of do's and don'ts that lawmakers should consider when developing a data protection framework.

BACKGROUND

Have you ever filed taxes or made a phone call? Do you own a smartphone? Have you ever used the internet? Do you have a social media account or wear a fitness tracker? If the answer is yes to any of these questions, it means that you have been sharing personal information, either online or off, with private or public entities, including some that you may never have heard of. Sharing data is a regular practice that is becoming increasingly ubiquitous as society moves online. Sharing data does not only bring users benefits, but is often also necessary to fulfill administrative duties or engage with today's society. But this is not without risk. Your personal information reveals a lot about you, your thoughts, and your life, which is why it needs to be protected.

The right to protection of personal data is very closely interconnected to, but distinct from, the right to privacy.

More than 160 countries refer to the right privacy in their constitutions, but the understanding of what "privacy" means varies from one country to another based on history, culture, or philosophical influences.[2] This explains why the way to protect privacy might differ from one country to another even if many legal traditions center the protection of privacy on the right to respect for private and family life, home, and correspondence. Data protection, on the other hand, is not always considered as a right in itself. The 28 member states of the European Union are an exception, as they have recognised data protection as a fundamental right in the 2001 EU Charter.[3] However, the protection of personal data is of paramount importance in our

[1] Access Now, General Data Protection Regulation – what tidings do ye bring? https://www.accessnow.org/general-data-protection-regulation-what-tidings-do-ye-bring/
[2] See results provided by the Constitute Project https://www.constituteproject.org/search?lang=en&key=privacy
[3] See Article 8 of the EU Charter of Fundamental Rights, 2001. http://www.europarl.europa.eu/charter/pdf/text_en.pdf

increasingly digital society. It is often recognised through binding frameworks at the national, regional, and international level, and in many places where it is not yet codified, lawmakers are in the process of doing so. We believe this should happen as quickly as possible.

Protecting personal data, or personally identifiable information (PII), means establishing clear rules that any entity that processes your information must follow. This is not a new concept, as data protection laws have been in place in many countries around the world for more than 40 years, but these laws are becoming increasingly important as people are sharing more data and companies' data collection and use skyrockets. The first data protection law was passed in 1970 by the German federal state of Hesse.[4] A few years later, the US developed the "fair information practices" that have influenced modern data protection laws, even though the US has never followed up with a codified legal framework for data protection at the federal level, instead adopting sector-specific laws.[5] Then came the first country-wide laws protecting personal data, in Sweden, Germany, and France, before international organisations such as the Council of Europe adopted international frameworks. The Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data — also known as Convention 108 — was adopted in 1980 and became open for signature in 1981.[6] In 1980, the Organisation for Economic Cooperation and Development (OECD) also developed its privacy guidelines.[7] Since its adoption, the Convention 108 has been ratified by all 47 member countries of the Council of Europe, and by Mauritius, Senegal, Uruguay, and, most recently, in 2017 by Tunisia.[8] The Convention 108 had a pivotal role in the adoption of the first Europe-wide data protection law in 1995.[9] Today, hundreds of countries around the world have adopted general or sectoral data protection laws.[10]

In addition to the frameworks in place, there are countries currently considering data protection legislation: Tunisia, India, Japan, South Korea, Brazil, and Argentina, to name but a few.[11] For some of these countries, it would be their first data protection law. Access Now has worked on data protection legislation across the world since 2009, and in particular, on the EU reform that led to the adoption of the General Data Protection Regulation.[12] The EU and its member states have a long data protection tradition and it is often considered a standard-setter in this area, which means that many countries are interested in replicating the GDPR in their own jurisdictions. There are important lessons to be learned from the negotiations of the GDPR, many positive and some negative. From our experience, we have created a list of do's and don'ts that lawmakers around the world should consider when developing a data protection framework.

[4] Hessische Datenschutzgesetz,Original version dated from 7 October 1970. (GVBl. I S. 625).
[5] See EPIC, the code of fair information practices. https://epic.org/privacy/consumer/code_fair_info.html
[6] Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, 1981. http://www.coe.int/web/conventions/full-list/-/conventions/treaty/108
[7] See Privacy International, Data Protection. https://www.privacyinternational.org/node/44
[8] Access Now, Tunisia ratifies Convention 108 and affirms commitment to the protection of personal data https://www.accessnow.org/tunisia-ratifies-convention-108-affirms-commitment-protection-personal-data/
[9] Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, 2015. https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf
[10] See Privacy International, Data Protection. https://www.privacyinternational.org/node/44
[11] Tunisia national authority for the protection of personal data. Projet de loi relative à la protection des données personnelles, 2017. http://www.inpdp.nat.tn/Projet_PDP_2017.pdf
[12] European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

DO'S

Below you will find 10 recommendations for policymakers to follow when developing a data protection law. These 10 steps are individually and collectively necessary to ensure open negotiations and the adoption a user-centric framework.

1 ENSURE TRANSPARENT, INCLUSIVE NEGOTIATIONS

Governments and decision makers must ensure that negotiations of data protection frameworks are conducted in an open, transparent, and inclusive manner. This means conducting public consultations and expert roundtables, publishing negotiating texts and allowing comments from all interested parties with reasonable deadlines, and providing feedback on received comments. In all stages, meaningful participation from civil society groups must be ensured, and all meetings of decision makers with industry, NGOs, and consumer groups must be made public in an easily accessible registry. Maximum transparency around lobbying should accompany the process. Due weight should be given to input from civil society, to redress the inevitable imbalance in number of voices compared with industry.

Experience from the GDPR negotiations

The GDPR negotiations were conducted in accordance with the EU legislative process. This process is fairly transparent and generally ensured the publication of draft proposals, opinions, reports, amendments, and legal opinions of all EU institutions on any piece of legislation being discussed. Some improvements can however be made to this legislative process. First, there should be more accountability in the earliest drafting stage of legislation. Through a FOIA request, Access Now has for instance obtained an email revealing how the Home Affairs department of the European Commission (DG Home) had been working alongside the US administration during the early stages of the privacy reform effort.[13] In addition, the trilogue — the final stage of the negotiations between all EU institutions — is notoriously opaque. Access Now has joined efforts led by European Digital Rights (EDRi) in calling for reforms of the process for years.[14] Because of the lack of transparency during that stage, the public is kept in the dark at the most crucial point in the negotiations; that is, when lawmakers come together to agree on a final compromise text that will become binding after the EU institutions rubber-stamp it.

External stakeholders seeking to influence negotiations should also abide by principles of transparency and accountability. The GDPR negotiations were subjected to an unprecedented lobbying effort during which industry representatives aimed to weaken existing data protection standards and to prevent proposals from strengthening users' rights. The influence of certain industries and foreign companies became visible as lawmakers copied and pasted amendment proposals from lobbying proposals.[15] In that instance, advocacy groups were able to help the public compare the language proposed by lobbyists to the text proposed by lawmakers.[16] This process allowed the public to comment meaningfully on these proposals and helped fight influence via secret backroom dealings. Proposing amendments is not necessarily a shady activity, but it must be done in a transparent manner. People must know where these proposals are coming from and lobbyists should always indicate their affiliation on their proposals and make them available to the public.

[13] Access Now, Big brother's little helper inside the European Commission https://www.accessnow.org/big-brothers-little-helper-inside-the-european-commission/
[14] Access Now, EU "trilogues" consultation: A foot in the door for transparency https://www.accessnow.org/eu-trialogues-consultation-foot-door-transparency/
[15] Access Now, Privacy under siege: Unprecedented lobby efforts against the Regulation are revealed https://www.accessnow.org/privacy-under-siege-unprecedented-lobby-efforts-against-the-regulation-are/
[16] See LobbyPlag initiative http://lobbyplag.eu/compare/overview

2 DEFINE AND INCLUDE A LIST OF BINDING DATA PROTECTION PRINCIPLES IN THE LAW

Any framework aiming to protect personal information must include a clear definition of personal and sensitive data. The level of protection should correspond with the sensitivity of each category of data. Sensitive data should be defined to include genetic and biometric data, as well as communications content and metadata, as this information reveals particularly sensitive personal traits. This means that a data protection framework can also include specific measures for the protection of data exchanged during communications and related privacy provisions to guarantee the confidentiality of communications.

Together with clear definitions, the eight following principles are at the core of data protection frameworks.[17] Put together, these interconnected principles lay down the necessary measures that any data protection framework which seeks to effectively protect users' rights should include. The effective codification of these principles requires the development of a set of users' rights, legal basis for data processing, data security measures, oversight mechanisms, obligations for entities processing data, and of measures enabling the transfer of data to third countries.

1. **Fairness and lawfulness:** Personal data shall be processed fairly and lawfully which means that information should be processed on a clear legal basis, for a lawful purpose, and in a fair and transparent manner so that users are adequately informed about how their data will be collected, used, or stored, and by whom.

2. **Purpose limitation:** Personal data shall be collected and processed only for a specified and lawful purpose. This purpose shall be specific, explicit, and limited in time. Data shall not be further processed in any manner incompatible with that purpose.

3. **Data minimisation:** Personal data collected and used shall be limited to what is adequate, relevant, and not excessive in relation to a specific and defined purpose.

4. **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date. Users shall have the right to erase, rectify, and correct their personal information.

5. **Retention limitation:** Personal data processed for any purpose shall not be kept for longer than is necessary.

6. **Users' rights:** Personal data shall be processed in accordance with the rights of users such as the right to access or right to erasure (See point 4).

7. **Integrity and confidentiality:** Personal data shall be processed in a manner that ensures state-of-the-art security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8. **Adequacy:** Personal data shall not be transferred to a third country or territory, unless that country or territory ensures an adequate level of protection for the rights and freedoms of users in relation to the processing of personal data. Data protection frameworks shall provide for mechanisms enabling the free flow of data between countries while safeguarding a high level of data protection.

Experience from the GDPR negotiations

The eight data protection principles come largely from international standards, in particular the Convention 108 and the OECD guidelines.[18] These data protection principles are considered "as minimum standards" for the protection of fundamental rights by countries that have ratified international data protection frameworks. These principles should be the basis of any data protection framework and are present in a large number of data protection laws around the world, from the EU Data Protection Directive from 1995, the GDPR, and most data protection laws that are in place in Latin America.

[17] See UK Information Commissioner's Office, Data Protection Principles https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/
[18] Organisation for Economic Cooperation and Development, September 1980. Guidelines governing the protection of privacy and transborder flows of personal data. https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf

3 DEFINE LEGAL BASIS AUTHORISING DATA TO BE PROCESSED

Any data protection law must clearly define the legal basis under which users' personal data can be processed. Any entity, public or private, seeking to process personal data must abide by at least one of the legal bases provided for in the law. These usually include the execution of a contract, compliance with a legal obligation, and a user's consent.

Consent shall be defined as an active, informed, and explicit request from the user. It must be freely given and the user must have the capacity to withdraw consent at any time. This means, for instance, that pre-ticked boxes would not qualify as valid consent. In addition, companies cannot deny a user access to a service for refusing to share more data than strictly necessary for the functionality thereof. Otherwise, consent would not be freely given.

Experience from the GDPR negotiations

The GDPR allows for six bases for processing personal data from contract to consent. [19] The definition of consent was strengthened and clarified during the negotiations compared to the definition provided for in its predecessor, Directive 95/46. The GDPR indicates that consent must be "a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication" of the user. However, the GDPR also authorises the processing of data for so-called "legitimate interest" purposes defined by the entity using the information. This provision greatly limits users' control over their personal information as they are often unaware of any data collection or processing when entities rely on legitimate interest (see more on legitimate interest in point two of the "Don'ts" section).

4 INCLUDE A LIST OF BINDING USERS' RIGHTS IN THE LAW

Protecting users' data protection and guaranteeing their control over their personal information requires establishing a series of binding rights to exercise:

1. **Right to access** enables users to obtain confirmation from services and companies as to whether personal data concerning them have been collected and are being processed. If that is the case, users shall have access to the data, the purpose for the processing, by whom it was processed, and more.
2. **Right to object** enables users to say "no" to the processing of their personal information, when they have not given their consent to the processing of their data nor signed a contract. This right to object applies to automated decision-making mechanisms, including profiling, as users have the right not to be subjected to the use of these techniques.
3. **Right to erasure** allows users to request the deletion of all personal data related to them when they leave a service or application.
4. **Right to rectification** allows users to request the modification of inaccurate information about them.
5. **Right to information** ensures that users receive clear and understandable information from entities processing their personal data, whether these entities have collected this information directly or received it through third parties. All the information provided to the user shall be provided in concise, intelligible, and easily accessible form, using clear and plain language. This information shall include details about data being processed, the purpose of this processing, and the length of storage, if applicable. The entities shall provide their contact details and an email address to allow users to contact them in case there are issues.
6. **Right to explanation** empowers users to obtain information about the logic involved in any automatic personal data processing and the consequences of such processing. This right is crucial to bring accountability and transparency in the use of algorithms to make decisions that impact users' lives.
7. **Right to portability** enables users to move certain personal data they have provided from one platform to another offering similar services. To facilitate this process, interoperability between services shall be encouraged.

[19] See Article 6. European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Although this list is not exhaustive, these rights must be provided for by law, and not left to the discretion of entities using the data. Users shall be able to exercise any of these rights free of charge.

Experience from the GDPR negotiations

The GDPR provides users with all mentioned rights, free of charge. The provisions enshrining those rights set detailed obligations on entities processing data to implement, provide for, protect, and respect these rights.[20]

The GDPR is an important step in ensuring that users can freely exercise their right to data protection. However, to ensure that all measures will be effective, there should be further effort to raise awareness about the existence of the law and its content. Governments, public authorities, companies, and NGOs should work jointly to achieve that goal.

Finally, the exercise of certain rights such as the right to portability and the right to explanation are particularly relevant in the era of Big Data and artificial intelligence. However, the full realisation of these rights will not take place without the cooperation of private entities developing algorithms, products, and services. We must ensure that engineers will create the necessary tools to enable the execution and enjoyment of these rights. For instance, a right to portability means nothing if platforms are not interoperable.[21] Similarly, a right to explanation can only exist if employees of companies relying on algorithms fully understand their functioning, and if they know why an algorithm is being used, what data are used in the algorithm, what data are created by the algorithm, and what variables the algorithm uses to make a decision. Given the limited language of the GDPR on that right, several academics are putting into question even the legal existence and the feasibility of such a right.[22] It seems clear that the GDPR intended to create such an avenue for users but it will be necessary to get further guidance from data protection authorities and stakeholders on how to interpret the text in practice. In short, creating such rights is positive but the conditions for the exercise of those rights must also be developed.

5 DEFINE A CLEAR SCOPE OF APPLICATION

The rights and principles established in a data protection law ensuring users' protection shall apply at all times. This means, for instance, that if an entity is offering a public or private service that involves the processing of data that targets users in the EU, users' rights encompassed under EU law shall apply.

In the digital age, it can be difficult for legislators to ensure sufficient protection of personal data and the rights of users without applying the principle of extraterritoriality. To understand the benefits of the extension of the jurisdictional scope of data protection, we need to look at the issue not from an "establishment" perspective (where is the entity located?) but from a user's perspective (where is the user and where is the user from?). The objective of human rights law, such as data protection frameworks, is first and foremost to protect individuals at all times. It is therefore logical to ensure that users' rights are respected no matter where the entities using people's data are located.

[20] See Chapter 3. European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[21] Article 29 Working Party on Data Protection, Guidelines on data portability. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf
[22] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, University of Oxford, Oxford Internet Institute. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469

Such application of the territorial scope also has the potential to raise the level of protection for users globally if companies and authorities start implementing data protection and privacy measures in their daily practices worldwide. In terms of competition, such jurisdictional measures can avoid a race to the bottom in terms of protection, whereby certain industries would decide to relocate their companies outside a country to avoid applying user-protective measures.

It is important to note however that extending the jurisdictional scope of a piece of legislation is not without risk and should be carefully considered by lawmakers. Conflicts of laws could arise and certain states could seek to extend the scope of rights-harming measures outside their borders using the same justification. Furthermore, not every entity processing data around the world knows about every country-specific law. It is often unclear whose obligation it is to inform businesses and individuals about their respective obligations and rights. Awareness-raising campaigns shall be conducted to ensure that entities around the world know their obligations. In order for data protection laws to properly function, public authorities need the mandate and resources to carry out public education. Civil society can and should have an active role in the process, in particular to empower people to enforce their rights.

Extending the scope of jurisdiction is not a one-size-fits-all solution and specific criteria should be established in data protection laws to limit bad copies or harmful consequences. Lawmakers should for instance clearly indicate under which scenarios the law applies outside their borders, to which actors specifically, what enforcement mechanisms will be in place, and provide users, companies, and authorities with clear avenues for remedies.

Finally, obligations under data protection law shall clearly apply to both the private and public sector. Public authorities are increasingly collecting individuals' information, getting access to private-sector databases, or otherwise building large databases of personal data. This processing shall be subject to clear obligations for the protection of individuals' personal information, the same way that processing by private entities is regulated.

Experience from the GDPR negotiations

The GDPR extends the territorial scope of the law compared to the 1995 Data Protection Directive. The GDPR applies to any companies and authorities established in the EU but also to entities established outside the EU if those are either processing personal information in connection with the offering of goods or services to, or monitoring of behaviour of, users who are in the European Union.[23] This important change in the scope of application of the law reflects the evolution of EU jurisprudence. For many years, courts in the EU battled with large tech companies that refused to comply with local data protection laws, based on issues of jurisdiction. Google and Facebook have repeatedly argued that they are not covered by data protection laws, for example, in Spain or Belgium, as they were not formally established in these countries. They took this position despite the fact that the companies were mining and monetising personal information from users in these countries.[24] [25] By extending the territorial scope of application, the GDPR sought to respond to these loopholes in protection for users and achieve legal certainty for users. This change is not however without challenges as it is not clear how EU data protection authorities will be able to conduct enforcement actions toward entities located outside the EU and therefore adequately protect rights.

[23] See Article 3. European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[24] Court of Justice of the European Union, Judgement in Case C-131/12, Google Spain SL vs Mario Costeja González, 13 May 2014. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5eb572d024de249578524881c67efe5ec.e34KaxiLc3eQc40Lax-qMbN4PaN0Te0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=-first&part=1&cid=574499

[25] Reuters, Facebook wins privacy case against Belgian data protection authority, June 2016. https://www.reuters.com/article/us-facebook-belgium-idUSKCN0ZF1VV

6 CREATE BINDING AND TRANSPARENT MECHANISMS FOR SECURE DATA TRANSFER TO THIRD COUNTRIES

Data protection frameworks are designed to ensure the free flow of data by establishing adequate mechanisms for data transfer and effective safeguards for users' rights. These mechanisms must be put under strict and transparent oversight and include effective remedies to ensure that the rights of users travel with the data.

Experience from the GDPR negotiations

Under the GDPR, cross-border data transfer outside the European Economic Area may only take place if the transfer is made to a country that has been accorded an adequacy status or when a lawful data transfer mechanism is in place.[26] The GDPR provides for more mechanisms for transfer than the Directive from 1995 through codes of conduct and certification schemes. This approach provides companies with greater flexibility. Effective oversight and enforcement of these mechanisms will be crucial to ensure that users' rights remain protected during and after transfer.

Regarding adequacy, the European Commission has the power to determine whether a third country ensures an adequate level of protection by reason of its domestic law or due to the international commitments into which it has entered, thereby permitting data to be exported to that jurisdiction. Any country can apply for an adequacy decision which will launch a review process conducted at the sole discretion of the EU Commission. Currently, the European Union has granted adequacy to the following countries[27]: Andorra, Argentina, Canada, Switzerland, Faroe Island, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, United States of America, and Eastern Republic of Uruguay. Adhesion to the Council of Europe Convention 108 is of particular importance in that respect, and is one of the elements taken into consideration in the assessment of the adequacy granting.

In 2016, the US lost the arrangement called Safe Harbour on which its adequacy determination was based due to non-compliance with EU fundamental rights law.[28] The validity of several elements of its new arrangement (EU-US Privacy Shield) continues to be under scrutiny.[29] Other countries like Australia have been requesting an adequacy decision but have so far failed to meet the necessary requirements.[30] Finally, ongoing negotiations for review and new adequacy are currently taking place with Japan.[31]

[26] See Chapter 5. European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[27] EU Commission, Commission decisions on the adequacy of the protection of personal data in third countries http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
[28] Access Now, CJEU declares Safe Harbor invalid https://www.accessnow.org/cjeu-declares-safe-harbour-invalid/
[29] Access Now, Comments to EU Commission on Privacy Shield review https://www.accessnow.org/cms/assets/uploads/2017/07/AN-PSReviewResponse-1.pdf
[30] European Commission, DG Justice, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_country_report_b2_australia.pdf
[31] European Commission, Joint statement by Vice-President Andrus Ansip and Commissioner Věra Jourová on the dialogue on data protection and data flows with Japan, March 2017. http://europa.eu/rapid/press-release_STATEMENT-17-690_en.htm

7 PROTECT DATA SECURITY AND DATA INTEGRITY

To experience the benefits of the digital economy, users need to be able to trust the services they use online. Any data that are shared generates a risk. Therefore, it is increasingly important to ensure that privacy and data protection are considered by engineers in the design phase of product and services and that they are set to the highest standards of protection by default; this is the concept of data protection by design and by default. Those concepts should be spelt out in the law to require entities to adopt them.

Experience from the GDPR negotiations

The GDPR codifies the principles of data protection by design and by default which provides a large number of benefits, such as contributing to data security and integrity.[32] With privacy and data protection by design and by default, companies take a positive approach to protecting users' rights, by embedding privacy-protecting principles into both technology and organisational policy. Privacy and data protection becomes part of the company culture and accountability framework, rather than being a "simple" compliance element. This requires thinking about privacy and data protection from the beginning of the process of developing a product or service.[33] This approach can help companies save on development costs for products or services. Because engineers and development teams will have considered privacy and data protection at the outset of the development phase, there would be fewer adjustments that would have to be made when a legal team reviews the final product. It also reduces the risk of a company being sued for privacy violations or suffering reputational damage due to data leaks, as it would be able to demonstrate its commitment to users' rights. In short, moving from understanding privacy and data protection as a compliance issue to embedding privacy and data security by design and by default can help companies increase trust in their services.

8 DEVELOP DATA BREACH PREVENTION AND NOTIFICATION MECHANISMS

While data protection frameworks should encourage measures fostering data security and data integrity, data breaches can still take place. Measures to address, remedy, and notify users of such problems shall therefore be put in place. Data breaches have gained widespread attention as businesses of all sizes become increasingly reliant on cloud computing and online services. With personal and sensitive data stored on local devices and on cloud servers, breaching network and information security has become attractive to those seeking to expose or exploit private information or demand a ransom. Data breaches have existed for as long as individuals' private records have been maintained and stored. Before the digital era, a data breach could be something as simple as viewing an individual's file without authorisation, or finding documents that weren't properly disposed of.[34] With the digitisation of records and ever-growing personal data collection, the scale of data breaches has skyrocketed, putting users' personal information at greater risk.

[32] See Article 25. European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[33] For more information on Privacy by Design see Ann Cavoukian, Privacy by Design, the 7 Foundational Principles https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf
[34] Nate Lord, The history of data breaches, July 2017. https://digitalguardian.com/blog/history-data-breaches

To prevent and mitigate these risks, mechanisms for data breach notification and prevention of such breaches should therefore be developed, either within a data protection framework or in complementary legislation. High-profile incidents of personal data loss or theft across the globe have prompted wide debate on the level of security given to personal information shared, processed, stored, and transmitted electronically. In that context, gaining and maintaining the trust of users that their data are secure and protected represents a key challenge for organisations. The NGO Privacy Rights Clearinghouse have recorded 7,619 data breaches that have been made public since 2005 in the US alone.[35] This means that at least 926,686,928 private records have been breached in the US since then. IBM and Ponemon Institute report that in 2017 the global average cost of a data breach is $3.62 million.[36] While this cost has slightly decreased compared to last year, the study shows that companies are having larger breaches. Other studies estimate that the average cost of a data breach will be over $150 million by 2020, with the global annual cost forecast to be $2.1 trillion.[37] This means that preventing and mitigating data breaches is not only good for users, but also good for businesses in order to save costs.

Experience from the GDPR negotiations

Data breach notification requirements were introduced in the European Union for the electronic communication sector in 2002.[38] Further specific sectoral rules have been developed since then to serve until those measures are harmonised under the GDPR to facilitate compliance for organisations.

The measures adopted under the GDPR require an organisation to report a data breach "without undue delay" and where feasible within 72 hours after it becomes aware of the incident.[39] While it is clear that the objective of the measure is to ensure that data breaches are reported as quickly as possible, the language is vague. The GDPR then describes the steps that any organisation encountering a breach must follow and provides for the possibility of notifying users. Such notifications are positive from an accountability and transparency perspective and are also crucial to ensure that users can take appropriate action to secure their information and seek remedy if necessary. However, the GDPR leaves it up to organisations to determine whether to notify users of a breach based on their own risk assessment of users' rights and freedoms. Notification to users should be a requirement for any data breach of personal data, which includes not only subscriber information, but other personal data such as photos. Notification should be timely, easy to understand, and comprehensive, and remediation options should be clearly indicated and accessible. By leaving too much discretion to organisations, this provision falls short of empowering users to take control of their information. Organisations suffering a data breach have an obvious economic interest in downplaying the risks associated with a breach and not notifying users, which could result in unaddressed data protection violations. We encourage lawmakers around the world to avoid those shortcomings and develop unambiguous data breach prevention and notification mechanisms.

[35] Privacy Rights Clearinghouse, Data Breaches. https://www.privacyrights.org/data-breaches
[36] Ponemon Institute for IBM, 2017 Cost of Data Breach Study: Global Overview https://www.ibm.com/security/data-breach/
[37] The Experian, Data Breach Industry Forecast, 2015. https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf
[38] European Union, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML
[39] See Articles 33 and 34. European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

9 ESTABLISH INDEPENDENT AUTHORITY AND ROBUST MECHANISMS FOR ENFORCEMENT

No data protection framework can be complete without a robust enforcement mechanism which includes the creation of an independent supervisory authority (data protection authority — DPA — or commission). Even the best data protection law in the world would be close to meaningless without an authority having the powers and resources to monitor implementation, conduct investigations, and sanction entities in case of (repeated, neglected, or willful) data protection violations.

Sanctions should be proportionate to the violations and can be in the form of notice to action. Authorities can for instance request a company stop certain practices that violate users' rights to data protection, such as the failure to provide a privacy policy or selling users' sensitive information without their knowledge and consent.

While punitive fines need to exist, data protection authorities shall apply limited fines to companies, in particular small or medium enterprises (SMEs), that do not engage in significant data processing, do not have the means to understand their obligations to respect data protection law, and have made mistakes out of ignorance rather than malice. Government shall also conduct awareness-raising efforts in order to avoid situations where companies would be ignorant of the existence and relevance of data protection laws. Tunisia, which is currently discussing its first ever data protection law, is proposing a quite innovative gradual approach to sanctions which includes higher fines in cases of recidivism.[40] As a result, a company found to commit data protection violations for which it has already been sanctioned would receive a significantly higher fine.

Sanctions and fines however represent only a small part of the work of DPAs. The role of data protection authorities is of course to enforce data protection laws and conduct oversight but also to assist organisations in their compliance duties. This means that companies, public authorities, and NGOs shall cooperate with data protection authorities to understand each other's duties and obligations. Organisations should not hesitate to establish contact with their DPA which can provide them with resources and materials to help implement the law.

Finally, DPAs have the powers to launch independent investigations into organisations and to hear cases brought to them by individuals or NGOs. In that sense, DPAs act as a guardian for users' rights and can help protect fundamental rights. These authorities are however still largely unknown by users around the world. To further help protect users' rights, NGOs should be empowered to represent users and to independently bring cases in front of DPAs and courts. Governments shall also further promote the work of DPAs, explain their role, and provide them with an adequate budget to ensure that DPAs can fulfil their duties.

Experience from the GDPR negotiations

The European Union and its member states have had data protection laws for almost 30 years. Despite this, many companies were ignoring them due to the lack of enforcement powers for data protection authorities and the relatively low level of fines (up to 150.000€).[41] For years in Europe, legal advisers often advised companies not to comply with EU data protection law, as the risk of being fined was as low as the amount they would have to pay.[42] This blatant disregard for fundamental rights was addressed under the GDPR by raising the fine level to a maximum of 4% of the worldwide turnover of the company.[43] The enforcement powers and the functioning of the DPAs have also been clarified and harmonised. DPAs will now be gathered within a European Data Protection Board which allows them to, for instance, conduct joint investigations across different EU countries.

[40] Tunisia national authority for the protection of personal data. Article 211. Projet de loi relative à la protection des données personnelles, 2017. http://www.inpdp.nat.tn/Projet_PDP_2017.pdf
[41] European Union. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046
[42] See Panel discussion at Computer, Privacy and Data Protection, Brussels, 2015. https://www.youtube.com/watch?v=sikwHfoiylg
[43] See Chapters 7 and 8. European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

10 CONTINUE PROTECTING DATA PROTECTION AND PRIVACY

Having a comprehensive law is a great milestone, but it does not mean governments should stop here in the protection of personal data and privacy. New challenges to privacy and data protection are likely to emerge during implementation phases even if governments aim at making laws "future-proof." This means that a review process will likely be necessary, which is a great opportunity to update the law, address any potential issues with compliance, and provide additional clarity and legal certainty where needed.

It is also important to understand a data protection law as a floor and not a ceiling in the protection of users' rights. This means that organisations must comply with the law, as a minimum, but should also be encouraged to go beyond and take further actions to protect people's privacy. Similarly, depending on the structure and form of the government of a country, different approaches to data protection and privacy can be taken into account. For instance, in the US, the federal government should not prevent local governments and states from providing for user protections, in addition to the limited measures provided at the federal level, and refrain from using its power to preempt regional and local laws.[44] However, in the case of the European Union, member states shall avoid creating additional rules as this would risk fragmenting the harmonised high level of protection for users agreed under the GDPR.

Experience from the GDPR negotiations

Since 1995, EU member states have adopted different local data protection laws based on the benchmark provided by the EU Data Protection Directive. This EU law was completed at a time when only 1% of the population was online, and it was in urgent need of modernisation when the EU Commission proposed the EU General Data Protection Regulation in 2012.[45] It took almost five years of negotiations for lawmakers to agree to the new measures in the law which will become directly applicable from May 2018 (unlike a Directive, which needs to be transposed into national law, a Regulation is directly enforceable). All 28 national data protection laws will be replaced by this single law that provides for harmonised rights and rules across the EU. While this system works under the EU's legal order, it might not be the ideal scenario in other regions or countries. Supranational laws can be difficult to agree upon and might not necessarily be the best instrument to protect users. There is therefore no ideal model for a law but all data protection laws shall take into account all the points laid down in this paper.

[44] EPIC, Privacy preemption watch. https://epic.org/privacy/preemption/
[45] European Commission, Reform of EU data protection rules, 2012. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

DON'TS

Below you will find five recommendations for policy makers to follow when developing a data protection law. We advise caution on the following five elements which, if ignored, could limit the benefits of the proposed law or harm individuals' rights.

1 DO NOT SEEK BROAD DATA PROTECTION AND PRIVACY LIMITATIONS FOR NATIONAL SECURITY

Governments not only have an obligation but also a security interest in ensuring the protection of personal data, in particular when information is held by government agencies. In 2015, as the result of a cybersecurity incident in the US, 21.5 million records of federal employees and family members stored at the Office of Personnel Management were stolen.[46] As these types of incidents and attacks are increasing globally, countries have must take measures to better protect individuals' information.

Despite this, governments often seek limitations to data protection and privacy rights for their own use of personal data by asking for broad exceptions. These exceptions must be prevented and limited to clearly defined, necessary, and proportionate measures that include judicial oversight and accessible remedy mechanisms. Legislation should not give governments and public entities the capacity to shield themselves from the obligation to protect users' right to data protection. Countries have a security interest in safeguarding personal data held by government agencies.

Experience from the GDPR negotiations

The GDPR provides a list of reasons that member states can rely on to restrict users' rights and freedoms protected under the law, such as national security or defence.[47] While it is common to find provisions allowing states to restrict rights in every piece of EU and national legislation, the language of these provisions is often purposefully vague and can potentially cover a wide range of state activities. The GDPR for instance allows for restrictions of rights for broad and undefined "other important objectives of general public interest of the Union or of a Member State". Given the impact of such restrictions on users' rights and freedoms, they should be clearly defined and limited in law, subjected to strict transparency and oversight criteria, and be necessary and proportionate measures in a democratic society.

2 DO NOT AUTHORISE PROCESSING OF PERSONAL DATA BASED ON THE LEGITIMATE INTEREST OF COMPANIES WITHOUT STRICT LIMITATIONS

Companies often argue that they should have a right to collect and process user data, when this is their "legitimate interest", without having to notify users. Unless such exceptions are defined as being exceptions (not the case under the GDPR or the 1995 Directive) and narrowly defined (which is better achieved in the GDPR), this should not be allowed. Otherwise, this intrinsically contradicts the objective of data protection, which is to put users in control of their information. Such attempts to limit users' rights must be prevented.

[46] Patricia Zengerle, Megan Cassella, Millions more Americans hit by government personnel data hack, Reuters, 2015. https://www.reuters.com/article/us-cybersecurity-usa/millions-more-americans-hit-by-government-personnel-data-hack-idUSKCN0PJ2M420150709
[47] See Article 23. European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Experience from the GDPR negotiations

Organisations' legitimate interest is one of the legal bases that can be used to process personal data under the GDPR.[48] The core of data protection is users' control and predictability in the use of their data. The legitimate interest provision goes against these principles. Under "legitimate interest" an organisation is authorised to collect and use personal information without having to notify the concerned users. If you don't know that an entity holds data about you, how could you exercise your right to access the data or your right to object?

This provision was one of the most debated during the negotiations of the GDPR. Companies were defending a broad and vaguely defined provision for legitimate interest and civil society was trying to remove it or significantly limit its scope. Lawmakers tried to limit the impact of the provision in the last months of negotiations by including a requirement for companies to balance their legitimate interest with fundamental rights. While the intention is laudable, companies will conduct this assessment at their own discretion and users could be kept in the dark. The final result is satisfying for no one as businesses wanted even more flexibility than accorded in the text and corresponding recitals, and NGOs wanted clear limitations. We understand the need to provide companies with measures that allow them to conduct business, however, measures that prevent users from having control over their personal information shall be excluded as they contradict the spirit and objective of a data protection law.

3 DO NOT DEVELOP A "RIGHT TO BE FORGOTTEN"

The "right to be forgotten" or "right to de-list" emerges from EU data protection law including the "Google Spain" ruling.[49] This right allows users under certain circumstances to request search engines to de-list web addresses from results when a search is done using their names. This right should not be confused with the right to erasure which allows individuals to delete all personal data related to them when they leave a service or application. The right to erasure is essential to ensure user control over personal information. It also should not be conflated with any take-down measure since the right to be forgotten developed under EU jurisprudence does not require or request any online content to be removed from the web or from search engine indexes.

The way several governments internationally have, accidentally or otherwise, misinterpreted the right to de-list or sought to extend its scope to limit freedom of expression or of information poses a significant threat to human rights. Courts and legislators around the world have demonstrated significant interest in developing measures to establish a "right to be forgotten" which significantly deviates from the approach developed by EU

[48] See Article 6. 1. (f). European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[49] Court of Justice of the European Union, Judgement in Case C-C-131/12, Google Spain SL vs Mario Costeja González, 13 May 2014. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5eb572d024de249578524881c67efe5ec.e34KaxiLc3eQc40Lax-qMbN4PaN0Te0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=-first&part=1&cid=574499

courts, mandating content removal.[50] [51] [52] Any so-called right to be forgotten measure that would lead to deletion of online content is a gross misinterpretation of the right. Under no circumstances must the right to de-list be applied to enable the removal of online content. Similarly, data protection authorities shall not be authorised to request the deletion of online information without the oversight of a judge that can ensure that all fundamental rights, including the right to free expression and freedom to access information, are respected.

Access Now opposes any development of such a "right to be forgotten". If however a right to de-list similar to the one in place in the EU were to be considered by lawmakers, Access Now has identified a series of legal safeguards that lawmakers must put in place to further mitigate the risks of abuse and harms to human rights.[53]

Experience from the GDPR negotiations

The right to be forgotten was added to the right to erasure in the GDPR.[54] The right to be forgotten codifies the jurisprudence of the EU Court of Justice in the "Google Spain" case.[55] The court has developed a set of criteria for search engines to consider when they receive a de-listing request. Search engines must grant a de-listing request only if the personal information included in the designated web address is "inadequate, irrelevant, or no longer relevant, or excessive", and only if the information does not pertain to a public figure or is not of public interest. However, information or links shall not be removed from the search index. They must remain accessible when users conduct searches using terms other than the name of the individual making the de-listing request. Importantly, the GDPR also clarifies that information shall not be de-listed if it is necessary for exercising the right of freedom of expression and information.

Despite those safeguards, further guidance from the EU and its member states is necessary to ensure that search engines do not "over- or under-comply" with the law and the ruling. Uncertainty regarding the geographical scope of application of the right to be forgotten has for instance led to new legal proceedings.[56] For their part, search engines should be more transparent about the criteria they have been using internally to deal with these requests.

Finally, in the current implementation of the right to de-list in the EU, access to remedy is limited. The only form of recourse that a user has is the opportunity to challenge a search engine's decision to deny a request to de-list. There should be more clarity on existing avenues for remedy, and these should be extended.

[50] Access Now, O direito ao esquecimento no Brasil: quais os riscos para os direitos humanos? https://www.accessnow.org/o-direito-ao-esquecimento-no-brasil-quais-os-riscos-para-os-direitos-humanos/
[51] Access Now, Documento de posición: El "derecho al olvido" y su impacto en la protección de los Derechos Humanos https://www.accessnow.org/documento-de-posicion-el-derecho-al-olvido-y-su-impacto-en-la-proteccion-de-los-derechos-humanos/
[52] Access Now, In India, the "right to be forgotten" is in the hands of the Delhi High Court https://www.accessnow.org/india-right-forgotten-hands-delhi-high-court/
[53] Access Now, Understanding the right to be forgotten globally, September 2016 https://www.accessnow.org/cms/assets/uploads/2016/09/Access-Not-paper-the-Right-to-be-forgotten.pdf
[54] See Article 17. European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[55] Access Now, FAQ on the right to be forgotten, 2014. https://www.accessnow.org/cms/assets/uploads/archive/docs/GoogleSpainFAQRtbF.pdf
[56] Access Now, Only a year until the GDPR becomes applicable: Is Europe ready? https://www.accessnow.org/year-gdpr-becomes-applicable-europe-ready/

4 DO NOT AUTHORISE COMPANIES TO GATHER SENSITIVE DATA WITHOUT CONSENT

Given the importance of sensitive data, a higher level of protection than for the rest of personal data must be required to guarantee an adequate level of control for individuals. Therefore, the collection and processing of sensitive personal data shall only be authorised if individuals have given their explicit, informed consent and have the right to withdraw that consent subsequently.

Sensitive data encompasses a wide range of personal information such as ethnic or racial origin, political opinion, religious or other similar beliefs, memberships, physical or mental health details, such as genetic or biometric data, information about personal life and sexuality, or criminal or civil offences. The particular nature and relevance of this information means that users should always be able to control who gets access to and use of this information. As a result, the processing of sensitive information should only be authorised if users have freely given informed and explicit consent. To protect the essence of users' fundamental rights to privacy and data protection, no exception to these rules shall be allowed.

Experience from the GDPR negotiations

The GDPR requires organisations to obtain the explicit consent of the user for the collection of sensitive data as a general basis. While this is extremely positive, the law also authorises the collection and use of sensitive data without users' consent for some specific objectives, including "scientific or historical research purposes or statistical purposes".[57] This broad exception deprives users of control over their most intimate information and is even more problematic in the context of the growth of the e-health industry, large scale, Big Data analysis of political views, and more. If not limited, companies could get a hold of millions of pieces of sensitive information over the next few years, initially to conduct research and gather statistics on their products. In practice, it would be complex to conduct oversight of how organisations use these data, as users will not be informed. Users must be able to control which organisation has access to their health or voting records. This type of loophole must be avoided, or at least strictly limited by restricting the use of these data for research, and statistical research must be conducted in the public interest under strict oversight.

5 DO NOT FAVOR SELF-REGULATION AND CO-REGULATION MECHANISMS

For many years, companies and entities collecting data have been calling for regulation of privacy and data protection not through binding frameworks but rather through self- or co-regulation mechanisms that offer greater flexibility. Despite several attempts, there are no examples of successful non-binding regimes for the protection of personal data or privacy that have been positive for users' rights or, indeed, business as a whole.

As more data are being shared online and off, it is high time to develop mandatory frameworks for data protection and privacy all around the world to prevent or end these behaviours and put users back in control of their information. This will also enable the development of privacy-friendly innovation which is currently limited to a small number of companies that have undertaken a long-term engagement approach to protect their users instead of basing their business model in monetising users' private information.

[57] See Article 9.2.(j). European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Business models built on privacy can serve as a competitive advantage. In countries without overarching data protection laws, companies could innovate through their internal practices by developing voluntary safeguards and guidelines to improve people's trust in the digital economy. Even though self-regulation is inadequate as an enforcement mechanism and unsustainable for safeguarding individuals' rights, it can be beneficial in certain circumstances for both companies and individuals to adopt a voluntary framework in those countries. It cannot be relied upon, either from the perspective of individuals or businesses, due to the risk of "free-riding" by bad actors that will undermine privacy, trust, innovation and take-up of new products.

Experience from the GDPR negotiations

The European Union has a long experience of failed self- or co-regulation attempts in the area of free expression.[58] In the field of privacy and data protection, however, the EU has been a pioneer in the development of a high-level of protection for users. The GDPR is yet another example of that success. While far from perfect, the GDPR is a key instrument for the protection of fundamental rights in the EU, and reflects years of experience gleaned from the implementation of past laws and jurisprudence developed by courts. The GDPR creates clear and strong obligations for organisations but also introduces several accountability tools to further data protection rights such as the principles of data protection by design and by default and new provisions for company certification and industry-wide code of conduct schemes. Such tools aim to develop a vision of data protection beyond mere compliance with the law and encourage innovation in the field.

[58] EDRi, Human rights and privatised enforcement https://edri.org/wp-content/uploads/2014/02/EDRi_HumanRights_and_PrivLaw_web.pdf

CONCLUSION

Access Now wholeheartedly supports the development of local, regional, and international frameworks for the protection of personal data. These frameworks must be user-centric and focus on safeguarding and strengthening rights, while delivering clear and predictable rules for public and private entities to comply with. Last, but not least, we cannot highlight enough the importance of comprehensive and robust enforcement mechanisms overseen by an independent authority to ensure that the proposed protections are fully functional.

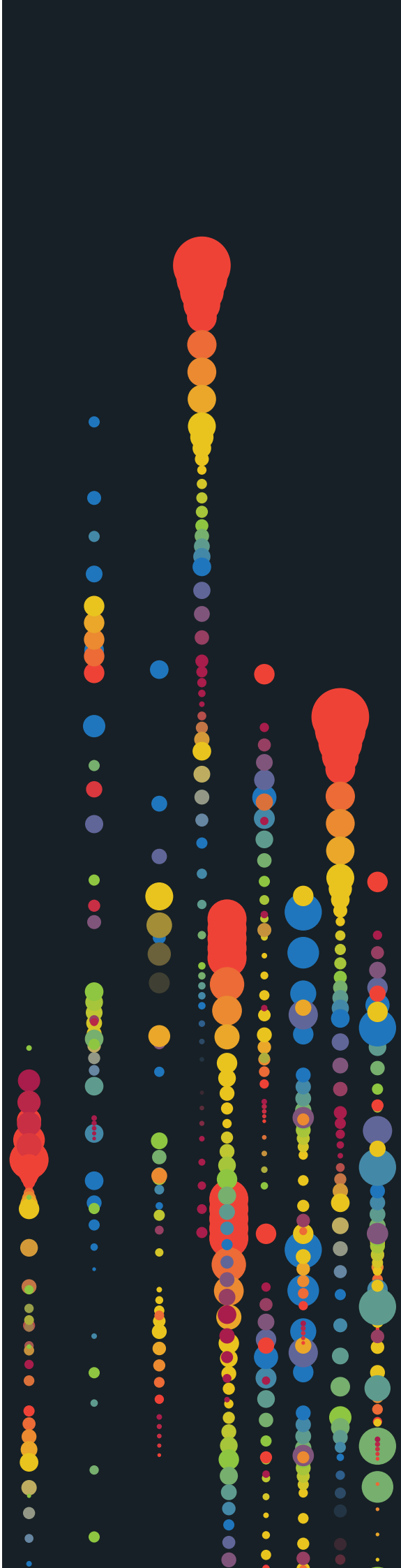
Protecting data protection globally has been a long-time area of focus for Access Now, and it continues to be one of our highest priorities. Among other issues, our team is actively engaged in the implementation of the GDPR, the reform of the data protection legislation in Argentina, and negotiations in India and Tunisia for developing a first data protection law.

CREATING A DATA PROTECTION FRAMEWORK:
A DO'S AND DON'TS GUIDE FOR LAWMAKERS

November 2018

This paper is an Access Now publication.

For more information, please visit: **https://www.accessnow.org,** or
contact: **Estelle Masse** | Senior Policy Analyst | **estelle@accesnow.org**



accessnow

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

https://www.accessnow.org

Annexure III

access

JULY 2015

UNIVERSAL IMPLEMENTATION GUIDE FOR THE INTERNATIONAL PRINCIPLES ON THE APPLICATION OF HUMAN RIGHTS TO COMMUNICATIONS SURVEILLANCE

A PRODUCT OF ACCESS

accessnow.org

The primary authors of this guide are Amie Stepanovich and Drew Mitnick. Access and the authors would like to thank the following individuals for their valuable input, assistance, and feedback in the preparation of the guide:

Walid Al-Saqaf
Kevin Bankston
Roxana Bass
Jochai Ben-Avie
Brittany Benowitz
Deborah Brown
Jack Bussell
Fabiola Carrion
Alberto Cerda
Cindy Cohn
Hanni Fakhoury
Tomaso Falchetta
Susan Freiwald
Mike Godwin
Natalie Green
Elonnai Hickok
Arne Hintz
Martin Husovec
Tamir Israel
Zeke Johnson
Lee Kaspar
Priya Kumar
Joy Liddicoat
Susan Morgan
Carly Nyst
K.S. Park
Alexandrine Pirlot de Corbion
Katitza Rodriguez
Naureen Shah
Sarah St. Vincent
Amos Toh
Francisco Vera
Timothy Wagstaffe
Kate Westmoreland
Cynthia Wong

We would also like to thank current Access staff who contributed substantial time to the completion of this document: Brett Solomon, Peter Micek, Raegan MacDonald, Estelle Masse, Javier Pallero, Michael Carbone, and Rian Wanstreet.

This guide has been updated slightly as of July, 2015.

Table of Contents

I. Introduction

This Implementation Guide was created to help bridge the gap between developing The International Principles on the Application of Human Rights to Communications Surveillance ("the Principles") and putting those principles into practice.

The Principles provide a framework for assessing human rights obligations and duties in the commission of communications surveillance. Access, the Electronic Frontier Foundation, and Privacy International led a broad consultation process to develop the Principles, which were launched in July 2013. They have subsequently been endorsed by more than 400 civil society organizations, and have been referenced in debates on legislative reform in several countries and regions.[1]

This guide shows government agents, judges, lawyers, and others who are involved in processing government requests for user data how to apply the Principles to each stage of the process. It walks through five steps for acquiring and processing such data, giving implementing examples for applying the Principles to each step:

- **Step One**: Government Application for Information;
- **Step Two**: Judicial Consideration;
- **Step Three**: The Search;
- **Step Four**: Appeals and Remedies; and
- **Step Five**: International Cooperation.

Below, we explore the legal framework for privacy and surveillance, and explain the "Principles approach" to creating standards for protecting human rights.

a. Legal framework on privacy and surveillance

Privacy is one of our most important rights — not only is it inherently valuable, it is also essential for the protection and promotion of other fundamental rights such as the freedoms of expression, movement, assembly, thought, and religion.[2] The right to privacy is recognized in international conventions and reflected in many countries' national

[1] *See, e.g.*, Report and Recommendations of the President's Review Group on Information and Communications Technology, *Liberty and Security in a Changing World*, Dec. 12, 2013, fn. 120, available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; Annual Report of the Inter-American Commission on Human Rights, Dec. 31, 2013, *available at* http://www.oas.org/en/iachr/docs/annual/2013/informes/LE2013-eng.pdf.

[2] *See* Frank La Rue, *Report of the Special Rapporteur to the on the promotion and protection of the right to freedom of opinion and expression*, U.N. Doc. A/HRC/23/40 (April 17, 2013), available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

constitutions and domestic laws.[3] Under international law, the right to privacy is framed as the right not to be "subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence."[4]

Following up on a December 2013 resolution by the United Nations General Assembly, the Office of the High Commissioner for Human Rights (OHCHR) published a report, "The Right to Privacy in the Digital Age," in July 2014.[5] The report, which repeatedly cites to the Principles, noted, "there is universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice."[6] In December 2014, a new UN General Assembly Resolution called upon States to review procedures, practices, and legislation to ensure that the right to privacy was upheld in commission of communications surveillance and asked for the Human Rights Council to consider establishing a special procedure on the right to privacy — such a procedure was adopted in March 2015 and a special rapporteur on the right to privacy was established.[7]

The right to privacy implicates certain necessary procedural and substantive safeguards.[8] The OHCHR report concluded that international law provides a "clear and universal framework for the promotion and protection of the right to privacy," but also found that many states evinced "a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight."[9]

---

[3] International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]; European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, Nov. 4, 1950, 213 U.N.T.S. 2889 [hereinafter ECHR]; American Convention on Human Rights art.11, Nov. 21, 1969, 1144 U.N.T.S. 143 [hereinafter ACHR]; see, e.g., The Charter of Fundamental Rights and Freedoms (Constitutional Amendment) Act 2011 (Jamaica), s.13(3)(k); Constitution of the Federative Republic of Brazil, art. 5; Constitution of the Republic of South Africa, s.14.

[4] ICCPR art. 17. Article 11(2) of the ACHR states that "No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation." Article 8 of the ECHR provides more direct guidance about the nature of permissible interferences; *see also Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Martin Scheinin, U.N. Doc. A/HRC/13/37, para. 17 (Dec. 28, 2009), available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf ("The permissible limitations test, as expressed in the general comment, includes, inter alia, the following elements: (a) Any restrictions must be provided by the law (paras. 11-12); (b) The essence of a human right is not subject to restrictions (para. 13); (c) Restrictions must be necessary in a democratic society (para. 11); (d) Any discretion exercised when implementing the restrictions must not be unfettered (para. 13); (e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim (para. 14); (f) Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected (paras. 14-15); (g) Any restrictions must be consistent with the other rights guaranteed in the Covenant (para. 18)." (internal citations omitted)); UN Human Rights Committee (HRC), *CCPR General Comment No. 27: Article 12 (Freedom of Movement)*, Nov. 2, 1999, CCPR/C/21/Rev.1/Add.9, *available at http://www.refworld.org/docid/45139c394.html*.

[5] *The Right to Privacy in the Digital Age*, G.A. Res. 68/167, U.N. Doc. A/RES/68/167 (Jan. 21, 2014); *The Right to Privacy in the Digital Age: Rep. of the Office of the United Nations High Commissioner for Human Rights*, U.N. Doc. A/HRC/27/37 (June 30, 2014), available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

[6] *Id.* at 5.

[7] *The Right to Privacy in the Digital Age*, G.A. Res. 69/166, U.N. Doc. A/RES/66/166 (Feb. 10, 2015); *Human Rights Council Agenda Item 3, The Right to Privacy in the Digital Age*, 28th Sess., A/HRC/28/L.27 (Mar. 24, 2015) [final pending].

[8] ICCPR art. 17, Declaring both a substantive right to privacy and procedural rights under the law.

[9] *Supra*, note 5, at 16.

Applying these concepts to real world situations has always been difficult. Modern technologies have compounded these challenges by making surveillance cheaper and easier while further blurring the privacy rights to be protected. Further complicating matters, laws, regulations, and formal procedures often move too slowly to keep pace with the newest technologies.

In June 2013, UN Special Rapporteur Frank La Rue issued a very timely report on government Communications Surveillance. Mr. La Rue concluded that, despite the clear existence of rights in international human rights law,[10] these laws and procedures are not sufficiently nuanced to provide clear guidance to individuals and governments when applying them in individual cases.

The Principles started to fill this gap, and this guide is intended to accompany the Principles and continue where they left off. It draws on existing human rights jurisprudence and explains how obligations apply to electronic communications surveillance for law enforcement, national security, or any other regulatory purpose.

b. The Principles approach

Discussions about surveillance and access to user information are often fragmented and based on artificial and outdated distinctions. Whether or not they should, separate dialogues often occur in the contexts of national security and local criminal contexts. The Principles bridge this divide by focusing on the impact of surveillance on the user, rather than the nature of the information or the motivation of the government agent. They set out standards to protect users' rights, regardless of whether the government seeks access for law enforcement, national security, or intelligence-gathering purposes.

The Principles recognize that increasingly individuals trust more and more of their information in the hands of third parties, a process that often involves storage and transfers across multiple jurisdictions. However, this does not necessarily mean that individuals expect that their most personal information could or should be considered public or that government could be granted unfettered access to it. In fact, recent events demonstrate just how vast the discrepancy is between how users and governments interpret personal expectations of privacy. These users are now mobilizing to demand that government laws and practices be accountable and respect human rights.[11] The systematic violation of human rights undermines true national security and jeopardizes international peace and security.[12]

[10] La Rue, supra note 2.

[11] *See, e.g.*, Stop Watching Us (Sept. 17, 2014), StopWatching.US.

[12] UN Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, Sept. 28, 1984, E/CN.4/1985/4, *available at* http://www.refworld.org docid/4672bc122.html; see also OTI report by Danielle Kehl.

II. How to Use this Guide

To help readers understand and apply the Principles in a variety of contexts, we have developed a set of standard defined terms that appear throughout the following sections. These terms are capitalized so that you can easily look them up in the glossary below, Terminology in this Guide.

Following the glossary, you will find a shortened version of the International Principles on the Application of Human Rights to Communications Surveillance, so that you can make easy reference to them (the full text of the Principles appears in Appendix A).

In addition to guiding you step-by-step through the five stages of handling government requests for users' data (Section III), describing each step, at the end of each step, we provide implementing examples.

Finally, we provide a helpful checklist of the considerations that we examine herein (Appendix B), as well as two case studies (Appendices C and D), to develop a more complete picture of what surveillance conducted that protects human rights would resemble.

a. Terminology in this guide

Account

is a record or collection of records created due to the interaction between a Target and another entity, which may be a user, organization, network, company, or any other party.

Adjudicator

is an official of a Judicial Authority with authority to act with the force of law.

Application to Conduct Communications Surveillance or Application

is a document filed with a Judicial Authority seeking authority to conduct Communications Surveillance.

Communication

is any imparting, receipt, or exchange of information or data between a user and any other entity or entities, which may be any other user, organization, network, company, or any other party. The Communication includes both the content as well as any metadata concerning that Communication, including but not limited to subscriber information, the identity of the parties to any communications, biometric information, location information, IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications.

Communications Surveillance

encompasses the monitoring, intercepting, collecting, obtaining, analyzing, using, preserving, retaining, interfering with, accessing, or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future.

Court Order for Communications Surveillance or Court Order

is a document issued by a Judicial Authority authorizing the monitoring, intercepting, collecting, obtaining, analyzing, using, preserving, retaining, interfering with, accessing, or similar actions taken with regard to information that includes, reflects, arises from, or is about a person's communications in the past, present, or future.

Device

means any piece of mechanical hardware used by a Target to collect, transmit, store, or communicate information or to facilitate the collection, transmission, storage, or communication of information.

Emergency Circumstances

are those in which there is an imminent risk or danger to human life and for which standards are defined explicitly in public law.

Formal International Channel

is a process for the exchange of User Data between jurisdictions. Any Formal International Channel provides clear guidance on which laws apply in situations involving multiple jurisdictions, clearly defines Protected Information, requires judicial authorization for any access to Protected Information, applies a higher evidence threshold for more sensitive information, and provides clear guidance on sharing information under Emergency Circumstances.

Government Agent

means an agent, instrumentality, employee, contractor, or other person working on behalf of a government to conduct Communications Surveillance, and includes but is not limited to law enforcement agents, prosecutors, and national security officers.

Judicial Authority

is a competent and impartial government entity responsible for making determinations related to Communications Surveillance which is separate and independent from authorities legislating or conducting Communications Surveillance.

Legitimate Aim

is a predominantly important legal interest that is necessary in a democratic society, the primary purpose of which is not to infringe on any internationally recognized human right and the fulfillment of which does not discriminate on the basis of race, color, sex, language, religion, political or other opinion, national or social origin, property, birth, sexual orientation, or other status.

Necessary Information

is User Data that a Government Agent has identified as relevant to a Legitimate Aim and the Communications Surveillance of which represents the least intrusive means by which to investigate or pursue the Legitimate Aim.

Notice of Intent to Use Emergency Procedures

is advance, written notice of a plan to conduct Communications Surveillance when Emergency Circumstances exist which pre-empt the standard process to conduct Communications Surveillance. The notice must be provided to the same Judicial Authority which will receive and review the associated Application to Conduct Communications Surveillance.

Protected Information

is User Data that includes, reflects, arises from, or is about a user's communications and that is not readily available and easily accessible to the general public. This Implementation Guide applies exclusively and comprehensively to Protected Information.

Providers

refers to both content providers and service providers — companies and organizations that provide access to the Internet and related services. While these entities typically fall under separate legal regimes, the sensitive user information that they collect and store means they should safeguard user rights similarly against Communications Surveillance. "Providers" include:

- telecommunications carriers (e.g. America M6vil, Vodafone);
- information service providers (e.g. Comcast, Orange);
- interactive computer service providers (e.g. Google, Baidu);
- information content providers (e.g. BuzzFeed, BBC);
- applications and over-the-top service providers (e.g. Zynga, WhatsApp)

Repository

a record or collection of records created to store, process, or manage data by, for, or about a Target but is not necessarily generated by the Target's direct activity or communications.

Request for Assistance

is a written application for mutual legal assistance made pursuant to a Formal International Channel.

Request for Search or Request

is a written notice that a Judicial Authority has approved a Court Order for Communications Surveillance and identifying the specific Communications Surveillance that has been authorized. The Request for Search should include the identity of the Adjudicator having entered the Court Order and the requesting Government Agent, and all information on all available means of redress, remedy, or appeal.

Search

is Communications Surveillance according to a Court Order to Conduct Communications Surveillance or pursuant to the terms of a Notice of Intent to Use Emergency Procedures.

Target

is a User or other specific and identifiable entity identified as possessing Necessary Information and therefore subject to an Application to Conduct Communications Surveillance and any resulting Communications Surveillance authorized under a Court Order. A non-individual may be a Target in its own capacity but not for the purpose of obtaining access to its customers, users, or other individuals who are properly Targets in their own capacity.

User

is any single individual.

User Data

includes information or data to, from, created by, or about a User.

b. The Principles in short

The International Principles on the Application of Human Rights to Communications Surveillance provide a framework for assessing human rights obligations and duties when conducting Communications Surveillance.

For easy reference, following is a shortened version of the Principles (see Appendix A for the full version).

LEGALITY

Any limitation on the right to privacy must be prescribed by law.

LEGITIMATE AIM

Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society.

NECESSITY

Laws permitting Communications Surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a Legitimate Aim.

ADEQUACY

Any instance of Communications Surveillance authorized by law must be appropriate to fulfill the specific Legitimate Aim identified and effective in doing so.

PROPORTIONALITY

Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.

COMPETENT JUDICIAL AUTHORITY

Determinations related to Communications Surveillance must be made by a competent Judicial Authority that is impartial and independent.

DUE PROCESS

States must respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public.

USER NOTIFICATION

Individuals should be notified of a decision authorizing Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorization.

TRANSPARENCY

States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities.

PUBLIC OVERSIGHT

States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance.

INTEGRITY OF COMMUNICATIONS AND SYSTEMS

States should not compel service providers or hardware or software vendors to build surveillance or monitoring capabilities into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes.

SAFEGUARDS FOR INTERNATIONAL COOPERATION

Mutual Legal Assistance Treaties (MLATs) entered into by States should ensure that, where the laws of more than one State could apply to Communications Surveillance, the available standard with the higher level of protection for individuals should apply.

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS

States should enact legislation criminalizing illegal Communications Surveillance by public and private actors.

III. Implementing the International Principles on the Application of Human Rights to Communications Surveillance

Step One: Government Application for Information

1. Authority to make an application

Applications to Conduct Communications Surveillance must be made in accordance with the law.

Relevant principle(s): Legality

The ability for a Government Agent to conduct Communications Surveillance must be authorized by publicly available and discernable law that complies with international human rights laws. Such law must have been promulgated in a public forum and subject to open debate, and cannot be altered or otherwise construed by any secret document or opinion.[13] Government Agents must abide strictly by these provisions.

Implementing example:
General Comment 16 of the United Nations Human Rights Committee interpreting Article 17 states, "[t]he term 'unlawful' means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant."[14] "[R]elevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis."[15]

2. Necessity of a search

Communications Surveillance should only be requested when there is no less intrusive means that can be used.

Relevant principle(s): Necessity, Adequacy, and Proportionality

In order to conduct a Search to obtain Protected Information, a Government Agent must clearly demonstrate that Communications Surveillance is the least intrusive means that can be used to obtain Necessary Information in order to achieve an identified Legitimate Aim.

In order to do this, the Government Agent must specifically determine the scope of the Necessary Information. It is not enough that the Communications Surveillance is related to

[13] According to international standards, in developing Communications Surveillance laws, "[e]verybody should be informed and consulted in the process of law drafting" with limited exceptions. Provided information should clearly explain the issues addressed issues and extra precautions should be taken to ensure civil society involvement. *Transparency and Public Participation in Law Making Processes*, pg. 6-7, Organization for Security and Co-Operation in Europe, Oct. 2010, available at http://www.ecnl.org/dindocuments/381_Transparency%20in%20Law%20Making%20Eng.pdf.

[14] UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, April 8, 1988, *available at*: http://www.refworld.org/docid/453883f922.html.

[15] *Id.*

the Target, the Legitimate Aim, or the Account, Device, or Repository to be searched. The scope of the Communications Surveillance, instead, must be narrowly tailored to minimize the impact on other Protected Information.

Implementing example:
In the case of Chaparro Alvarez and Lapo Íñiguez, the Inter-American Court of Human Rights recognized that intrusions into privacy must be "appropriate to achieve the purpose sought...necessary, in the sense that they are absolutely essential to achieve the purpose sought and that, among all possible measures, there is no less burdensome one in relation to the right involved, that would be as suitable to achieve the proposed objective. Hence, the Court has indicated that the right to personal liberty supposes that any limitation of this right must be exceptional and...that the measures are strictly proportionate, so that the sacrifice inherent in the restriction of the right to liberty is not exaggerated or excessive compared to the advantages obtained from this restriction and the achievement of the purpose sought."[16]

Implementing example:
In Canada, §186(1)(b) of the Criminal Code provides that wiretapping may be accepted as an appropriate investigative tool where "other investigative procedures are unlikely to succeed."[17] In R v Araujo, the Supreme Court of Canada interpreted this in light of "... two potentially competing considerations: enabling criminal investigations and protecting privacy rights."[18] Accordingly, in order to satisfy the investigative necessity test, the police must establish that there is no other reasonable or less intrusive method of investigation.

3. Format of the application

Applications to Conduct Communications Surveillance should be made in writing to a Judicial Authority and:
- clearly identify the requesting agency and officer; and
- certify as to the truth and accuracy of the information contained in the application.

Relevant principle(s): Due Process

In order to access Protected Information, a Government Agent must submit a written Application to Conduct Communications Surveillance to a Judicial Authority. The Application must include the name of the Government Agent seeking access, his or her position, proof of his or her valid authority to present the Request, and his or her signature certifying the truth as to all included information.

[16] Chaparro Alvarez v. Ecuador, Judgement, Inter-Am. Ct. H.R. (ser. C) No. 170 (Nov. 21, 2007), *available at* http://observatoriovihycarceles.org/en/hiv-and-prison-menu/jurisprudence-prison-menu.raw?task=download&fid=505.
[17] Criminal Code, R.S.C. 1985, c. C-46 (Can.).
[18] *R v Araujo* [2000] 2 S.C.R. 992 (Canada), *available at* https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1830/index.do.

The procedures by which a Government Agent files an Application to Conduct Communications Surveillance should be clearly delineated in law.[19] Regardless of his or her identity or position, a Government Agent must provide transparency into and take responsibility for the information contained in the Application (see below) in accordance with all applicable laws, including laws presumed within this Guide, and under the penalty of perjury.

Implementing example:
In the United States a certification would take the form of an affidavit presented under oath that accompanies the issuing warrant, subpoena, or other instrument.

4. Content of application

An Application to Conduct Communications Surveillance should clearly state:

- The Legitimate Aim that the Communications Surveillance seeks to accomplish and the Necessary Information sought to achieve that Legitimate Aim;
- The Target of the Communications Surveillance (if unknown, then all available facts related to the Target's identity should be included so that a reasonable person may verify that the Application relates to a valid Target);
- The relevant laws authorizing the requested Communications Surveillance; and
- The precise scope of the requested Communications Surveillance.

Relevant principle(s): Legitimate Aim, Adequacy, Necessity, and Proportionality

All Applications to Conduct Communications Surveillance should explain what Legitimate Aim is served by the Communications Surveillance, the exact Necessary Information needed to achieve the Legitimate Aim, and why. The Application should explain why Communications Surveillance, including access to Protected Information, is required. The Application should also identify, to the fullest extent possible, the Target of the Communications Surveillance. A new Application should be submitted for every additional Target.

Finally, an Application must precisely describe the scope of the Communications Surveillance requested. A proper description of the scope should describe the Account, Device, or Repository subject to Communications Surveillance, the particular database thereon, any extraneous Protected Information expected to be accessed, the methodology to be used, the relevance of the Necessary Information to the identified Legitimate Aim, and the specific timetable, either in the time span over which they can acquire data or the period for which they have access to a certain Account, Device, or Repository.

[19] In common law countries, the application will typically be made by the law enforcement officer, whereas in civil law countries it is more common that the application be made by prosecutors. The Principles accommodate either system.

Implementing example:
The Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights (ICCPR) explain circumstances in which limitations can be placed on international human rights, including on the basis of national security.[20] Although non-binding, the Siracusa Principles are considered persuasive interpretation of the ICCPR.

5. Burden of proof

The Application to Conduct Communications Surveillance should contain enough information to demonstrate to the Judicial Authority that:

- the Communications Surveillance will produce Necessary Information;
- the Necessary Information sought is contained in the identified Account, Device, or Repository subject to Communications Surveillance; and
- the identified scope of the Communications Surveillance (see above) is defined as to produce no more Protected Information than required to obtain the Necessary Information.

Relevant principle(s): Legitimate Aim, Adequacy, and Proportionality

Applications to Conduct Communications Surveillance must be reasonably supported and may not be part of a "fishing expedition." A Government Agent must provide sufficient detail in the Application to Conduct Communications Surveillance to demonstrate a sufficient nexus, defined clearly in public law, between the Account, Device, or Repository to be subject to Communications Surveillance and the Necessary Information identified. In order to meet this burden, a Government Agent must include the alleged acts and/or omissions that support the need for the Communications Surveillance and the lawfully acquired facts that provide the evidentiary basis for believing that the acts and/or omissions occurred. The facts in the Application must further support a finding that, to the greatest extent possible, the scope of the Communications Surveillance and the methodology to be used in the Search are appropriate and narrowly tailored to encompass the least amount of Protected Information in order to obtain the Necessary Information.

Implementing example:
In the U.S., in order to obtain a warrant, evidence must meet the standard of "probable cause" as required by the Fourth Amendment to the U.S. Constitution. "Probable cause" has been explained as a "fair probability that contraband or evidence of a crime will be found in a particular place."[21]

An application for a warrant should contain sufficient information to establish "probable cause" to believe that the evidence sought constitutes evidence of the commission of a criminal offence or represents contraband, the fruits of a crime or criminally derived

[20] UN Commission on Human Rights, *supra* note 11.
[21] *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

property. The Application for a Search warrant should also include reasonable grounds to believe that the evidence sought can be found at the specified location, along with a detailed description of the items to be seized, with sufficient specificity so as to identify them (for example, asking for specific records between certain limited dates or for specific personal property associated with the underlying crime).

6. Emergency procedures

Emergency procedures may be used under specific, enumerated Emergency Circumstances. In Emergency Circumstances, a Notice of Intent to Use Emergency Procedures must be filed before any Communications Surveillance may be undertaken. Then, an Application to Conduct Communications Surveillance must be filed with the Judicial Authority as soon as possible after the initiation of the Search. If the application is denied then Search must promptly stop and all information must be immediately destroyed.

Relevant principle(s): Legality, Due Process, and Safeguards Against Illegitimate Access

In a situation where Communications Surveillance is otherwise authorized and when the law provides specifically for their use, emergency procedures may be used to expedite the initiation of Communications Surveillance. Emergency procedures should only be used in situations where Emergency Circumstances are determined to exist. In Emergency Circumstances, a Notice of Intent to Use Emergency Procedures must be filed prior to the start of the Communications Surveillance that gives notice that emergency procedures are to be used. However, if the Government Agent determines at any time that the Emergency Circumstances no longer exist, they must immediately cease the Search and return to non-emergency protocols.

The Notice of Intent to Use Emergency Procedures must clearly demonstrate what Emergency Circumstances exist that require the use of emergency procedures, and how those Emergency Circumstances meet the established standard. As soon as possible after the Search is initiated, a full Application to Conduct Communications Surveillance must be filed within a timeframe established by law, preferably within 24-72 hours from the initiation of the Search.

Mere risk of flight or destruction of evidence should never be considered as a sufficient basis to justify the use of emergency procedures.

Implementing example:
In the Republic of Korea, whenever there is an imminent risk of a serious crime being committed which may cause death or serious injuries to individuals, the investigating officer may conduct electronic surveillance without the authorization of the court. However, he or she must obtain judicial approval of the use of surveillance within 36 hours of the surveillance having begun.[22]

[22] Protection of Communications Secrets Act, art. 8, Act n. 6626/2002, Jan. 2002, *available at* https://www.imolin.org/doc/amlid/Republic_of_Korea_Protection_of_Communications_Secrets_Act.pdf.

Step Two: Judicial consideration

1. Adjudicating authority

An Application to Conduct Communications Surveillance must be made to a Judicial Authority that is impartial, competent, and independent.

Relevant principle(s): Competent Judicial Authority, Due Process, and Public Oversight

All Applications to Conduct Communications Surveillance require authorization by a Judicial Authority, which makes a determination on the content and sufficiency of the Application.

The Judicial Authority must be impartial, competent, and independent.[23] As explained in the Principles, this means that the Judicial Authority must be separate from the branch to which the Government Agent conducting Communications Surveillance belongs, conversant in issues related to the legality of Communications Surveillance, the technologies used to do so, and international human rights laws, and have adequate resources in exercising the assigned functions.

Adjudicators must have access to sufficient training to be able to issue informed decisions, as well as access to individuals with technical, procedural, and other necessary expertise. Proceedings in front of the Judicial Authority should be public and transparent, and its decisions must be published. States should dedicate adequate funding to ensure that an Adjudicator can respond to Applications in a prompt manner, as required in time-sensitive investigations and particularly to limit the instances when it is necessary to use emergency procedures.

Implementing example:
In interpreting the Article 17 obligation on States not to unlawfully or arbitrarily interfere with individuals' privacy, the Human Rights Committee has stressed the need for independent, impartial adjudication.[24]

[23] Domestic and international laws enshrine the right to access to justice and fairness in a legal proceeding, with judges playing a prominent role in guaranteeing these protections. *See* La Rue, *supra* note 2, for discussion of the importance of an independent judiciary to adjudicate issues impacting on freedom of expression.

[24] *See e.g.*, UN Human Rights Committee, *Concluding Observations of the Human Rights Committee Poland*, UN Doc. CCPR/C/79/Add.110, July 29, 1999, *available at* http://www.un.org/en/ga/search/view_doc.asp?symbol=CCPR/C/79/Add.110 ("As regards telephone tapping, the Committee is concerned (1) that the Prosecutor (without judicial consent) may permit telephone tapping; and (b) that there is no independent monitoring of the use of the entire system of tapping telephones."); *UN Human Rights Committee, Concluding Observations of the Human Rights Committee*, UN Doc. CCPR/C/79/Add.89, April 6, 1998, *available at* http:llwww.un.orglenlgalsearchlview_doc.asp?symbol=CCPRlCl79lAdd.89. ("The Committee recommends that steps be taken to ensure that interception be subject to strict judicial supervision and that the relevant laws be brought into compliance with the Covenant").

Implementing example:
In Sweden, signals intelligence that is intended to collect intelligence data must be approved by the Defense Intelligence Court, which ensures that the surveillance is lawful and could not be conducted in a less invasive manner. The Court also evaluates if the value of the surveillance outweighs human rights intrusions.[25]

2. Sufficiency of application

A Court Order for Communications Surveillance should only issue if a Judicial Authority determines that the substance of an application for Communications Surveillance meets the legal, substantive, and procedural requirements, including the burden of proof.

Relevant principle(s): Legality, Due Process, Legitimate Aim, Necessity, Proportionality, and Adequacy

A Court Order to Conduct Communications Surveillance must only issue if the Judicial Authority determines that the Application meets all legal and substantive requirements and all procedures have been followed, as set out above. The Adjudicator has a separate, independent responsibility to ensure that an Application to Conduct Communications Surveillance contains all of the required information as spelled out above, including sufficient detail so that the Adjudicator, without additional information, can determine that the evidentiary standard is satisfied (see below).

When assessing the content of the Application to Conduct Communications Surveillance, the Adjudicator must ascertain that the information it is based upon is credible and was lawfully acquired. Any information that does not meet this standard cannot be considered when determining if the Government Agent has met his or her Burden of Proof.

3. Evidentiary standards

A Court Order to Conduct Communications Surveillance should only issue if an Adjudicator determines that the Communications Surveillance is necessary (see above) and that there is a sufficient nexus connecting the specific Account, Device, or Repository with the identified Necessary Information. The Court Order should only authorize Communications Surveillance that is narrowly tailored to encompass no more Protected Information than is required to serve a Legitimate Aim.

Relevant principle(s): Proportionality, Legitimate Aim, Adequacy, and Necessity

The Judicial Authority may only authorize Communications Surveillance that represents the least intrusive means to obtain identified Necessary Information in order to serve an identified Legitimate Aim.

[25] The Law Library of Congress, *Foreign Intelligence Gathering Laws*, December 2014, 34, *available at* http:llwww.loc.govllawlhelplforeign-intelligence-gatheringlforeign-intelligence-gathering.pdf.

Before a Court Order may issue, the Judicial Authority must also determine that the Government Agent has demonstrated a sufficient nexus between the Account, Device, or Repository on which Communications Surveillance is to be performed and the Necessary Information sought and that the scope of the Communications Surveillance is narrowly tailored to encompass no more Protected Information than is required to obtain the Necessary Information.

Implementing example:
In the U.S., in order to obtain a warrant, evidence must meet the standard of "probable cause" as required by the Fourth Amendment to the U.S. Constitution. "Probable cause" has been explained as a "fair probability that contraband or evidence of a crime will be found in a particular place."[26]

An application for a warrant should contain sufficient information to establish "probable cause" to believe that the evidence sought constitutes evidence of the commission of a criminal offence or represents contraband, the fruits of a crime or criminally derived property. The application for a Search warrant should also include reasonable grounds to believe that the evidence sought can be found at the specified location, along with a detailed description of the particular items to be seized, with sufficient specificity so as to identify them (for example, asking for specific records between certain limited dates or for specific personal property associated with the underlying crime).

4. Format and content of court order

A Court Order to Conduct Communications Surveillance should be in writing, and should include the:

- name of the Judicial Authority, the identity of the issuing Adjudicator, and the date the Court Order issues;
- law(s) under which the Court Order is issued
- methodology of the Search to be employed;
- scope and duration of the authorization; and
- the underlying Application to Conduct Communications Surveillance

When an Application to Conduct Communications Surveillance involves novel or unique factual or legal issues, the Adjudicator should also issue a written opinion explaining the issues and the rationale for the Adjudicator's decision to issue the Court Order.

Relevant principle(s): Proportionality, Adequacy, and Due Process

In order to facilitate an accountable process which is subject to public oversight, all Court Orders to Conduct Communications Surveillance must be in writing and clearly state the law or laws under which the Court Order issues. It should indicate the time and date that the

[26] *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

Court Order is issued, as well as the name and position of the authorizing Adjudicator. The supporting Application should be attached.

In addition, the Court Order must precisely describe the full scope of the authorization, including the exact Accounts, Devices, or Repositories subject to Communications Surveillance, and the particular database, as well as the time frame during which the Communications Surveillance may occur, the methodology for the Search, and the means and methods by which the Communications Surveillance may be conducted. In addition, whenever possible the Court Order should identify the particular databases to be searched and, at a minimum, the types of files that constitute Necessary Information should be listed.

The Adjudicator should tailor the terms of the Court Order to the substantive allegations in the Application to Conduct Communications Surveillance. The Court Order should never authorize a greater scope of Communications Surveillance than what is requested in the Application, and, when appropriate, the Adjudicator should sufficiently narrow the authorization so that Necessary Information is the only accessible Protected Information.

A Court Order to Conduct Communications Surveillance must specifically limit the time that Protected Information may be stored. Accordingly, the Court Order must provide for regular reports on all information obtained under the Court Order. This includes Protected Information that is not Necessary Information within the context of the identified Legitimate Aim or any Protected Information that is outside the scope of the Court Order. In addition, the Court order must require that Necessary Information within the scope of the Court Order may only be stored for a reasonable time, specified by the Adjudicator, not to outlast the resolution of the Legitimate Aim of the Communications Surveillance.

When an Application to Conduct Communications Surveillance involves novel or unique factual or legal issues, the Adjudicator should issue a written opinion explaining the issues and the rationale for the decision to issue the Court Order. The written opinion should be made public and the adjudicator should within it specifically explain any interpretation of the public law that was necessary in order to reach any relevant conclusion and the rationale behind that interpretation, citing to previous cases, opinions, or acts when appropriate.

5. Judicial oversight

It is the duty of the Judicial Authority to monitor the implementation of Court Orders to Conduct Communications Surveillance (or, in the case of a Government Agent who failed to seek or obtain a Court Order, some other Adjudicator). The Adjudicator should ensure that the State reports on the activities conducted under the Court Order.

Relevant principle(s): Necessity and Adequacy

The State should report to the Judicial Authority on all of the information, including Protected Information that was acquired during the Search so that the Judicial Authority can ensure that the implementing Government Agent complies with all terms of the Court Order.

The Government Agent must segregate Necessary Information. The Government Agent should report regularly to the Judicial Authority throughout the commission of the Search and during the entire time the State retains Protected Information obtained as a result of the Search. This reporting should take place not less than every 30 days, and during shorter periods of time for more invasive or broader Searches. The report must identify the Necessary Information sought, the scope of Protected Information obtained through the date of the report, the scope of Protected Information accessed that did not constitute Necessary Information, and the reason for the access.

Following the report, the Judicial Authority should order the destruction of any Protected Information that does not constitute Necessary Information unless there is evidence of impropriety and bad faith on behalf of the Government Agent. In this instance, the Adjudicator should order the immediate and effective quarantine of the information pending investigatory proceedings of the violating Government Agent. Further, the Adjudicator should order the destruction of all Protected Information, including Necessary Information, once it is no longer required for the Legitimate Aim for which it was obtained.

The report should also identify progress on compliance with the Judicial Authority's order for the destruction of Protected Information. The Government Agent must specify to the Judicial Authority the ways in which information has been destroyed. If the Adjudicator determines that the destruction process is being delayed or obstructed investigatory proceedings should be initiated to determine the reason for the delay or obstruction and appropriate discipline should be ordered, including, when appropriate, more frequent reporting.

6. Investigatory proceedings

Where investigatory proceedings are necessary, the Adjudicator who authorized the Court Order to Conduct Communications Surveillance (or, in the case of a Government Agent who failed to seek or obtain a Court Order, some other Adjudicator) should order the information relevant to the investigatory proceedings to be quarantined. A separate Adjudicator should be assigned to any investigatory proceedings and given stewardship over the relevant information. Once the investigatory proceedings are concluded the information should be destroyed.

Relevant principle(s): Legality, Competent Judicial Authority, Due Process, and Safeguards Against Illegitimate Access

Arbitrary and unlawful interferences with individuals' privacy are violations of human rights that undermine democratic governance.[27] Even minor interferences can constitute a grave violation when viewed in aggregate. Government Agents should be subject to investigatory proceedings for misconduct related to the Application for or commission of Communications Surveillance. In addition to the circumstances in this Implementation Guide where investigatory procedures are required, an Adjudicator should order investigatory proceedings for any instance where a Government Agent is determined to have violated the terms of the Court Order to Conduct Communications Surveillance. This should include when a Government Agent acts or orders another to act outside of the scope of the Court Order, knowingly accesses Protected Information that does not constitute Necessary Information, uses Protected Information for purposes other than the Legitimate Aim stated in the Application to Conduct Communications Surveillance, or violates any other substantive policy or procedure established by the Judicial Authority.

Investigatory proceedings should be public and should be assigned to an Adjudicator other than the Adjudicator who authorized the Court Order to Conduct Communications Surveillance. Upon any circumstance where investigatory procedures are required, the information that led to the need for investigatory procedures should be quarantined from any other information obtained in the commission of Communications Surveillance. During the course of the investigatory proceedings, stewardship over the relevant quarantined information should be given to the assigned Adjudicator. The information should never be used for any purpose outside of the investigatory proceedings. Once the investigatory proceedings have concluded, the Adjudicator should order all of the information destroyed.

Any Government Agent subject to investigatory proceedings should be prevented from continuing any work related to Communications Surveillance until the proceedings are closed. All work should be assigned to other Government Agents. The Adjudicator assigned to the investigatory proceedings should have authority to order any necessary discipline for the Government Agent, including suspension (with or without pay), termination, remuneration,

[27] La Rue, *supra* note 2

public apology, prolonged peer or judicial oversight and reporting, or other actions as enumerated by law. Investigatory proceedings should never pre-empt civil actions by an affected user. If a user opts to bring a civil action, the quarantine of the relevant information must continue through the civil proceedings before it is destroyed to ensure that it can serve any evidentiary purpose necessary (see the section on remedy for more information).

7. Emergency procedures

In Emergency Circumstances, a Judicial Authority must assess the Notice of Intent to Use Emergency Procedures and ensure that such Notice contains all necessary facts and allegations for the Adjudicator to determine if Emergency Circumstances exist. In these instances, the Judicial Authority should ensure that an Application to Conduct Communications Surveillance is filed within a reasonable timeframe after the Search is initiated and must review the Application under an expedited timeframe. The rationale for emergency procedures must be independently reviewed.

Relevant principle(s): Legality, Competent Judicial Authority, Due Process, and Safeguards Against Illegitimate Access

When a Judicial Authority receives from a Government Agent a Notice of Intent to Use Emergency Procedures, such Judicial Authority must receive the notice and ensure that it is immediately assigned to an Adjudicator. The Adjudicator must ensure that a complete Application to Conduct Communications Surveillance is filed within a reasonable timeframe after which the Search is initiated pursuant to the Notice. A reasonable timeframe should typically not be longer than 24-72 hours from the initiation of the Search.

The Adjudicator must consider both the content and the substance of the Notice of Intent to Use Emergency Procedures and the Application to Conduct Communications Surveillance on an expedited schedule.[28] If the Adjudicator denies the Application to Conduct Communications Surveillance, the Search must immediately cease and all Protected Information must be immediately destroyed, except in cases where the Adjudicator determines the Government Agent acted with impropriety and in bad faith, in which case the information should be quarantined pending investigatory proceedings. In egregious cases where the Application is found to be substantively lacking in form and/or substance, disciplinary sanctions should be pursued against the requesting Government Agent.

If the Application is accepted but modified, and the Adjudicator finds that the request for emergency procedures was valid, the Search should be immediately adjusted as to comport with the modified requirements, and Protected Information that no longer falls within the scope of the

[28] An example of adequate justification for the use of emergency procedures would be collecting location data to find a stolen car with a child locked inside. *TELUS Transparency Report 2013*, TELUS, 2013, *available at* http://about.telus.com/servlet/JiveServlet/previewBody/5544-102-1-6081/TELUS%20Transparency%20Repo rt%202013%20-English.pdf)

Court Order should be immediately destroyed, except in cases where the Adjudicator determines the Government Agent acted with impropriety and in bad faith, in which case the information should be quarantined pending investigatory proceedings. If the Application is accepted in any form, but the Adjudicator finds that an Emergency Circumstance, as defined by law, did not exist, emergency procedures were not appropriate for any other reason, or the Government Agent failed to provide sufficient justification, then the Search may continue. However, Protected Information subject to a Search prior to the issuance of the Court Order must be immediately destroyed (pending any necessary investigatory proceedings or accompanying civil actions) unless the Adjudicator makes a finding on the record that the Government Agent obtained the Protected Information, or inevitably would have done so, lawfully from an independent source.[29]

Implementing example:

The Indian Telegraph Act permits emergency collection when the Search is confirmed within seven working days. If not confirmed, the Search has to cease and further Collection may only occur with prior approval. A Review Committee meets to determine whether the Search was conducted in accordance to the law. If not, the Committee may end the Search and order the destruction of Collected data.[30]

[29] See Murray v. United States, 487 U.S. 583 (1988).

[30] *Law Enforcement Disclosure Report*, Vodafone, 42 (Jun. 2014), http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforce ment_disclosure_report.pdf.

Step Three: The Search

1. Scope of the search

A Search must comport with the specific terms of the Court Order and should not interfere with the integrity of a Provider's services.

Relevant principle(s): Necessity, Proportionality, Adequacy, and Integrity of Communications and Systems.

A Search must be precisely limited to the bounds of the Court Order to Conduct Communications Surveillance, or, in the case of the use of emergency procedures, to the reasonable terms of the Notice of Intent to Use Emergency Procedures entered prior to a Judicial Authority's determination on the related Application to Conduct Communications Surveillance. Any Government Agent that requires a Provider, as part of a Search, to reconfigure its architecture in any instance or turn over a code, password, or other piece of information that would provide access to a Device, Account, or Repository other than that belonging to the Target should be considered to have acted outside the scope of the Court Order.

Implementing example:
The Human Rights Committee has interpreted the requirement of "reasonableness" in article 17 of the International Covenant on Civil and Political Rights as implying that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."[31]

2. Costs

Costs associated with a Search should be borne by the State.

Relevant principle(s): Safeguards Against Illegitimate Access

The State should reimburse Providers for their reasonable costs incurred in conducting a Search. The basis for all costs should be specified in law. Providers should not be allowed to contract with a State for any costs that are above or in addition to the reasonable costs as established by law and determined by a Judicial Authority to prevent the creation of any perverse financial incentive to conduct Communications Surveillance. Reimbursement should be provided within a reasonable time period, not to exceed 30 days from the date the costs are incurred.

Implementing example:
In Switzerland, the federal government requires reimbursement for the costs of complying with surveillance requests. The government maintains a compensation chart based on the type of surveillance.[32]

[31] UN Human Rights Committee, *supra* note 17, at para 8.3.

[32] Regulation on fees and compensation for the monitoring of Mail and Telecommunications, SR 780.115.1, April 7, 2004, *available at* http://www.admin.ch/opc/de/classified-compilation/20032564/index.html

3. Request for search

A Request for Search issued to a Provider should be in writing, and should specify the User Data the State is requesting the Provider to remit, the legal basis for the Request, the name and contact information for the Government Agent issuing the Request for Search and the Judicial Authority who has authorized the Search, and a brief explanation of how the User Data sought is encompassed by the Court Order. Any documents necessary to understand the scope of the authorized Search should be attached to the Request for Search.

Relevant principle(s): Due Process and Public Oversight

Each Court Order to Conduct Communications Surveillance may produce more than one Request for Search, depending on the Providers implicated by the Court Order. A Request for Search should be specifically tailored to the Provider to which it pertains. Providers should only accept a Request for Search when it:

- is made in writing;
- explains the legal basis for the Request;
- identifies the official making the Request by name and title;
- specifies the permitted scope, duration, and methodology of the Search; and
- complies with all relevant legal or regulatory requirements.

The relevant Court Order to Conduct Communications Surveillance and the Application to Conduct Communications Surveillance should be attached, in full, to any Request for Search, as well as any other supporting documents filed that the Provider would need access to to understand the scope of the Request for Search.

4. User notification

The Target should be notified of a Search before it is conducted unless a Government Agent can demonstrate to a Judicial Authority that a delay is strictly necessary to prevent serious jeopardy to the purpose for which Communications Surveillance is authorized. Responsibility for notification resides with the State.

Relevant principle(s): User Notification

The State must notify a Target of a Court Order to Conduct Communications Surveillance in order to provide an adequate opportunity for the Target to challenge the validity of the Search and to assert any privileges that may attach to the information sought.

Notification should include information that would enable the Target to obtain legal guidance and, if he or she so chooses, to challenge the validity of the Court Order or the scope of the Search, including the Court Order itself and the Application to Conduct Communications Surveillance filed with the Judicial Authority.

In limited circumstances, notification may be delayed for a limited period of time upon request of the Government Agent and subject to approval by the Judicial Authority. Approval of a request for delayed notification should be subject to rigorous review and should never be automatic. Instead, delayed notification should only be granted if the Government Agent demonstrates that a delay is strictly necessary for preventing serious jeopardy to the purpose for which Communications Surveillance is authorized.[33] Potential considerations in making this determination may include:

- clear and present danger to the life or physical safety of an individual;
- flight from prosecution;
- evidence tampering; or
- witness intimidation.

A delay should only be granted for a well-defined, reasonable amount of time that should generally not exceed 30 days. If the delay needs to be extended beyond the initial period, the Government Agent must seek an extension from the Judicial Authority by showing:

- the Government Agent has complied with all requirements as enumerated in the Court Order to Conduct Communications Surveillance;
- a good faith effort to gather the Necessary Information within the time allotted and to resolve the circumstances which require a delay in notification; and
- demonstrable need for further extension.

Additional delays should be subject to the same process as the initial delay and must be subject to the same time limitations. Delays must not be granted indefinitely: the Target should be notified as soon as possible after the rationale for the delay has expired.

In addition to notification by the State, Providers should always be able to notify its users of Court Orders to Conduct Communications Surveillance.[34]

Implementing example:
In Japan, the Act on the Interception of Communications requires that the subject of intercepted communications must be notified of the interception within 30 days of the surveillance having been completed. Where an ongoing investigation might be compromised by such notice, a district court judge can extend the period of time within which the subject must be notified.

[33] *See, e.g. Klass v. Germany*, App. No. 5029/71, 2 Eur. H.R.Rep. 214 (1978).
[34] The role of companies in user notification is discussed further below.

5. Provider responses and challenges

Providers must only supply Protected Information in response to a Request for Search, supported by a valid Court Order. Where it appears that a Request for Search does not comply with the Principles and/or international human rights law obligations, Providers should demand further explanation and, where appropriate, challenge the legality of the Request.

Relevant principle(s): Legality, Legitimate Aim, Necessity, Adequacy, Proportionality, Competent Judicial Authority, and Due Process

Upon receipt of a Request for Search, a Provider must only provide Protected Information to the State as consistent with the most narrow construction thereof.[35] Any ambiguity should be resolved in favor of the Target. If the State and the Provider disagree as to an ambiguity, a Judicial Authority should resolve the disagreement and issue a clarifying addendum to the Court Order to Conduct Communications Surveillance and/or the Request for Search.

If a Request for Search is inconsistent with the law or this Implementation Guide a Provider should refuse to provide any Protected Information, and should instead file a legal challenge to the Request for Search.[36] If a Request for Search is consistent with local law, but inconsistent with international human rights law and/or made during a time of political turmoil, a Provider must evaluate the human rights risks, and the legal and operational risks. The Provider should also evaluate the potential to avoid or limit responses to any Request for Search through unilateral or multistakeholder advocacy, negotiation, litigation, or direct resistance.

Providers should assess the human rights situation in each operating environment in which they do or plan to do business. As part of these assessments, providers should engage with local and international stakeholders, independent human rights experts, and internal or external counsel with specific knowledge of relevant local laws and regulatory requirements. Providers should avoid pursuing business in operating environments in which users' access or human rights are subject to egregious restrictions inconsistent with international human rights law and the rule of law. Providers should conduct ongoing due diligence on human rights-related risks and review the appropriateness of continuing to operate in specific environments.

[35] A provider should treat User Data with a presumption that it is Protected Information. If a Request for Search rebuts this presumption and clearly applies only to non-Protected Information the Provider should act in the best interests of the User and with respect to the protections in this Implementation Guide.

[36] This section should be read in conjunction with the Access Telco Action Plan, which provides detailed guidance for telecommunications companies on respecting human rights.

Implementing example:
The Access Telco Action Plan offers 10 principles and implementation guidance for telecoms and ISPs to better prevent and mitigate any adverse human rights impacts.[37] The Plan counsels providers that, "Requests from governments and partners to restrict users' access, freedom of expression, or privacy should be presumptively rejected." To push back against requests that would restrict user rights, providers should, "Engage in unilateral and multistakeholder dialogue, and advocacy as needed, with governments and business partners." Joining with peer companies to resist particular requests has enabled providers to successfully reject government demands that threatened human rights.[38]

Implementing example:
Obligations under international human rights law attach to States, rather than directly to companies. However, Providers have a responsibility to respect human rights.[39] The UN Guiding Principles on Business and Human Rights explains:

> The responsibility to respect human rights is a global standard of expected conduct for all business enterprises wherever they operate. It exists independently of States' abilities and/or willingness to fulfil their own human rights obligations, and does not diminish those obligations. And it exists over and above compliance with national laws and regulations protecting human rights.[40]

The Guiding Principles on Business and Human Rights set out the nature of businesses' responsibilities, including obligations to conduct due diligence and provide effective access to remedy.

6. Data governance

Providers should use good data security hygiene and should not build surveillance or monitoring capability into their systems.

Relevant principle(s): Integrity of Communications and Systems and Transparency

Providers must be transparent with users regarding terms of use, privacy policies, and other forms of user guidelines or restrictions on user rights. This information should use accurate, clear, and accessible language and should be broken down by country and requesting entity.

In order to ensure that the exclusive means for States to gain access to User Data is through the process set out in this Implementation Guide, Providers should implement meaningful

[37] Access, *Telco Action Plan*, https://s3.amazonaws.com/access.3cdn.net/1f9ab2891a86f3f081_uom6iil1w.pdf
[38] Access, "Update: SMS finally unblocked in Central African Republic," 25 July 2014, https://www.accessnow.org/blog/2014/07/25/update-sms-finally-unblocked-in-central-african-republic.
[39] *See* Joseph, Sarah and Castan, Melissa (2013), *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary 3rd ed, p541.*
[40] *Guiding Principles on Business and Human Rights: Implementing the Protect, Respect, and Remedy Framework*, (2011), HR/PUB/11/04, p13.

data security practices. In the first instance, this should mean that Providers collect no more User Data than necessary in the ordinary scope of business. Further, the Provider should take meaningful steps to protect the User Data that it does retain, including User Data maintained at rest in databases or otherwise as well as User Data in transit to or from other users, companies, internal systems, or otherwise.

Data security should always be enabled by default and any critical updates should be pushed through to the user without altering any established privacy settings or access controls. When possible, the Provider should give the user the ability to control his or her own data without Provider access. Providers should always use security best practices and should undertake regular security audits to ensure that standards, systems, and technologies are up to date.

User Data should not be retained for longer than it is necessary for the Provider in the ordinary scope of business. When User Data is no longer necessary, it should be immediately and definitively destroyed, both that on the Provider's systems as well as the systems of any third party with which it has been shared. User Data should only be shared with third parties under valid, legitimate agreements that are necessary in the Provider's ordinary scope of business and communicated openly to the user in a manner that is easy to understand. Providers should not build surveillance or monitoring capability into their systems, or collect or retain User Data purely for State surveillance purposes.

7. Provider transparency

Providers should have the ability to publish granular statistics and policies on compliance with Request for Search and should do so. Wherever possible, providers should ensure that users are notified when their data are accessed.

Relevant principle(s): User Notification and Transparency

Providers should document and publish responses to Requests for Search and conduct regular reviews of these responses. Providers' transparency reports should include the:

- total number of each type of Request, broken down by legal authority, including the total number of Requests under emergency procedures;
- total numbers for each type of information sought;
- total number of users and accounts targeted;
- total number of users and accounts affected;
- total number of times delays in notification were requested, the number of times that a delay was granted, and the number of times a delay was extended;
- compliance rate, provided as a percentage of total Requests received and total Requests complied with;

- legal challenge rate, provided as a percentage of total Requests received and total challenged; and
- total amount of costs reimbursed to the Provider by the State, as allowed for above.[41]

In States where it is unlawful to provide this information, Providers should actively work for the ability to issue transparency reports.

Implementing example:
Many of the providers implicated in the NSA PRISM program, including Google, Facebook, Yahoo!, and Microsoft, release regular transparency reports. In 2013, these companies filed suit in the U.S. Foreign Intelligence Surveillance Court to be released from gag orders that prevent them from reporting more granular details about their involvement with state surveillance.[42] They eventually reached an out-of-court agreement with the Department of Justice,[43] but Twitter has argued that current parameters still violate the freedom of speech.[44]

Outside the U.S., many telecom providers, including Telstra,[45] TeliaSonera,[46] and Deutsche Telekom[47] have begun releasing transparency reports. In June 2014, Vodafone released "the most detailed transparency report ever,"[48] describing the laws governing surveillance and reporting in 29 countries, its own policies and procedures, and statistics on government requests.[49] In addition, the provider revealed related risks to user privacy and free expression, such as where provider's personnel are employed by government security agencies, and where governments enjoy direct access to its networks.

[41] Civil society groups, investors, and trade associations, such as those that participate in the WeNeedToKnow Coalition, agree that regulations must allow companies to report on the specific number of requests received, of users/devices/accounts/repositories affected, and of authorities involved. Access, "We need to know: companies, civil society call for transparency on surveillance," July 18, 2013, https://www.accessnow.org/blog/2013/07/18/tech-companies-and-civil-society-join-call-on-the-us-governmen t-to-issue-tr.
[42] Sam Gustin, *Tech Titans Press Feds in Battle Over NSA Transparency*, Time, Sept. 10, 2013, http://business.time.com/2013/09/10/tech-titans-press-feds-in-battle-over-nsa-transparency/
[43] Office of Deputy Attorney General, Letter to General Counsels, Department of Justice, Jan. 27, 2014, http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf.
[44] Jack Linshi, Twitter Pushing DOJ, FBI To Let It Disclose More Info on National Security Requests, Time, July 31, 2014, http://time.com/3063761/twitter-transparency-report/.
[45] Telstra Transparency Report, Telstra, March 2014, http://exchange.telstra.com.au/wp-content/uploads/2014/03/Transparency-Report_2014.pdf.
[46] TeliaSonera Transparency Report, TeliaSonera, Aug. 2014, http://www.teliasonera.com/en/sustainability/transparency-report.
[47] Deutsche Telekom, http://www.telekom.com/sicherheitsbehoerden.
[48] Peter Micek, *Vodafone reports on law enforcement access to user data, worldwide*, Access, June 6, 2014, https://www.accessnow.org/blog/2014/06/06/vodafone-reports-on-law-enforcement-access-to-user-data-worldwide.
[49] Law Enforcement Disclosure Report, Vodafone, http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_securit y/law_enforcement.html.

Step Four: Appeals and Remedies

1. Penalties for unlawful access

Laws should establish criminal penalties for unlawful access to Protected Information. States and companies should ensure that any user whose Protected Information is obtained in violation of international or domestic law has access to complaint mechanisms and to appropriate legal remedies. Unlawful access should be considered inherently harmful to the user to whom the information pertains.

Relevant principle(s): Safeguards Against Illegitimate Access

Legislation should prohibit unwarranted, unnecessary, disproportionate, or extra-legal attempts to conduct Communications Surveillance by either law enforcement agents or private actors.[50] Any Government Agent who is determined to have committed such a violation, or to have compelled another to do so, should be subject to investigatory proceedings (described above). Depending on the nature of the breach, additional appropriate penalties may include criminal sanctions, administrative discipline measures, and/or other direct fines to individuals who were involved in the wrongful Search.[51]

Users whose information is obtained without proper authorization and in violation of any domestic or international law or regulation should be able to seek redress.[52] Potential routes for remedy should include civil legal actions against the State, as well as non-judicial mechanisms, such as independent ombudsmen or national human rights institutions.

In order to ensure proper access to judicial relief, the wrongful Search should be considered inherently harmful to the user to whom the information pertains. In instances where a wrongful Search can be proven, both actual and punitive damages should be possible, as well as legal fees and restitution.[53] Improperly seized information should be returned to the user when appropriate and all copies should be quarantined under control of an Adjudicator and destroyed after investigatory proceedings or related civil actions have been closed.

[50] UN Human Rights Committee, *supra*, note 17

[51] This section should be read in conjunction with Access' Guide, *Forgotten Pillar: The Telco Remedy Plan*, May 2013, https://s3.amazonaws.com/access.3cdn.net/fd15c4d607cc2cbe39_0nm6ii982.pdf, which provides information on how telcos can meet their responsibility to provide access to remedy under the UN Guiding Principles on Business and Human Rights.

[52] *Guiding Principles on Business and Human Rights: Implementing the Protect, Respect, and Remedy Framework*, (2011), HR/PUB/11/04, Guiding Principle 25, ("As part of their duty to protect against business-related human rights abuse, States must take appropriate steps to ensure, through judicial, administrative, legislative or other appropriate means, that when such abuses occur within their territory and/or jurisdiction those affected have access to effective remedy"}.

[53] See John Ruggie, *Protect, Respect, and Remedy: a Framework for Business and Human Rights*, para. 25, A/HRC/8/5, April 7, 2008, available at http://www.reports-and-materials.org/sites/default/files/reports-and-materials/Ruggie-report-7-Apr-2008.pdf.

While the duty to provide remedy rests primarily with States, Providers should:

- incorporate the question of remedy into due diligence;
- implement accessible and secure grievance mechanisms; and
- respond quickly and effectively to user complaints.[54]

Providers should also adopt appropriate procedures to assist users in seeking remedy, such as investigating alleged breaches, preserving evidence, acknowledging and apologizing as appropriate, and providing compensation as necessary.

Implementing example:
Article 2(3) of the International Covenant on Civil and Political Rights states that each State Party has an obligation to "...ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity."[55]

2. Admissibility of unlawfully obtained information

Protected Information that is improperly obtained should not be admissible in any legal proceedings.

Relevant principle(s): Safeguards Against Illegitimate Access

Protected Information that is acquired in violation of domestic or international law, including the procedures in this Implementation Guide, should not be admissible in any legal proceeding (except for investigatory proceedings, as described above, or a related civil action). Evidence derived from such information should also be inadmissible except in proceedings against the responsible Government Agent to provide culpability (see above sections on investigatory proceedings and civil remedies).

Implementing example:
In Ireland, evidence obtained in breach of an accused person's constitutional rights is automatically excluded from criminal trial unless an adequate excusing circumstance exists.[56] Evidence obtained illegally but in compliance with the Constitution may also be excluded under a balancing test with factors that include the nature and extent of the Government Agent's illegality.[57]

[54] *Telco Remedy Plan, supra*, note 47 at 3.
[55] See also ECHR art. 13; ACHR art. 25
[56] People (DPP) v. Kenny (1990) IR 110.
[57] People (AG) v. O'Brien (1965) IR 142.

3. Government transparency

Governments should should regularly publish comprehensive statistics on Requests made and granted for access to Protected Information.

Relevant principle(s): Transparency and Public Oversight

States should publish regular transparency reports that inform the public about usage of Communications Surveillance authorities and practices and demonstrate how Government Agents comply with domestic and international laws.[58]

States' transparency reports should include the:

- total number of each type of Request, broken down by legal authority and requesting State actor, be it an individual, government agency, department, or other entity, and the number of Requests under emergency procedures;
- total number and types of responses provided (including the number of Requests that were rejected);
- total numbers for each type of information sought;
- total number of users and accounts targeted;
- total number of users and accounts affected;
- total number of times delays in notification were requested, the number of times that a delay was granted, and the number of times a delay was extended;
- compliance rate, provided as a percentage of total Requests received and total Requests complied with;
- legal challenge rate, provided as a percentage of total Requests received and total challenged;
- number of investigations into filed complaints and the results of those investigations; and
- remedies ordered and/or actions taken in response to any investigations.

Information should be explained quantitatively as well as qualitatively, so that any person is able to understand how Communications Surveillance takes place.

Implementing example:

In the criminal context, many States require their governments to publish statistics on the number of requests for surveillance made, granted, etc. For example, see §100e of the Criminal Procedure Code (Germany),[59] §170-172 of the Search and Surveillance Act 2012 (New Zealand),[60] and §195 of the Criminal Code (Canada).[61]

[58] State-produced transparency reports act in tandem with, and not separate from, provider reports. More information on what should be in a provider report is available above.

[59] Strafprozessordnung [StPO] [Code of Criminal Procedure], April 7, 1987, Bundesgesetzblatt (Federal Law Gazette), I at 1074, as amended, Section 100e "[Duty to Report]", *available at* http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0622.

[60] Search and Surveillance Act 2012, Section 170 "Annual reporting of search and surveillance powers by Commissioner" (N.Z.), *available at* http://www.legislation.govt.nz/act/public/2012/0024/latest/DLM3330254.html.

[61] Criminal Code (R.S.C., 1985, c. C-46), Section 195 "Annual report", *available at* http://laws-lois.justice.gc.ca/eng/acts/C-46/page-100.html#docCont..

In the security context, however, there has been little progress. In June 2014, the Office of the U.S. Director of National Intelligence (ODNI) released a transparency report that, as expected,[62] fell short of the standards established in the Principles.[63] A Google official pointed out that the ODNI report used imprecise language, making it "impossible" to cross-reference the report with service provider reports.[64] Moreover, the ODNI report failed to outline when and how the information was used, thereby "provid[ing] no basis for evaluating the utility or legitimacy of the surveillance activities."[65]

Other countries are even more opaque. Currently, not a single member of the Council of Europe releases a transparency report that includes requests made pursuant to national security-related investigations.

[62] Access, *Obama Administration continues to thwart meaningful transparency on NSA surveillance*, Aug. 30, 2013, https://www.accessnow.org/blog/2013/08/30/obama-administration-continues-to-thwart-meaningful-transpar ency-on-nsa-sur.
[63] *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year* 2013, IC on the Record, June 26, 2014, http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013.
[64] Richard Salgado, *A step toward government transparency*, Google Public Policy Blog, June 27, 2014, http://googlepublicpolicy.blogspot.com/2014/06/a-step-toward-government-transparency.html.
[65] Steven Aftergood, *ODNI Declassifies Data on Frequency of Surveillance*, Federation of American Scientists, June 30, 2014, http://fas.org/blogs/secrecy/2014/06/odni-frequency/.

Step Five: International Cooperation

1. Choice of laws and procedures

When a Government Agent seeks Protected Information from a foreign jurisdiction, a Request for Assistance must use publicly-available Formal International Channels.

Relevant principle(s): Safeguards for International Communication

Government Agents seeking access to Protected Information from a foreign jurisdiction must follow the appropriate Formal International Channel. The details of the Formal International Channel should be publicly available, including in each of the official or predominant languages of the State parties to the agreement to ensure accessibility for all users who are potentially affected by the agreements and practitioners charged with implementing them.[66]

Formal International Channels provide clear guidance on which laws apply in situations involving multiple jurisdictions. When faced with a choice, the Formal International Channel should require that the law with the higher standard for protecting individual rights applies. Formal International Channels should also specify the scope of Protected Information States may seek in a Request for Assistance and should require that Communications Surveillance conducted pursuant to a Request for Assistance conform to the standards set out in this Implementation Guide. Formal International Channels must provide clear guidelines for handling of Emergency Circumstances, including what constitutes an emergency, processes to be followed, documentation requirements, and the need for follow-up authorization.

Implementing example:
Mutual Legal Assistance Treaties (MLATs) are formal treaties that necessarily must be published and registered with the United Nations.[67] While arrangements for law enforcement cooperation or other less-than-treaty status arrangements are not included in this obligation, States should also make them publicly available.[68]

2. Authority for response

States must only comply with Requests for Assistance from foreign governments for Protected Information when the applicable Formal International Channel has been followed. Judicial Authorities should approve access to Protected Information when the Request for Assistance satisfies the law and meets the standards set out in this Implementation Guide.

Relevant principle(s): Safeguards for International Communication and Due Process

[66] Access is working to make MLATs more publicly accessible through [www.mlatinfo.org]
[67] U.N. Charter art. 1.
[68] *See* e.g., Rush v Commissioner of Police [2006] 150 FCR 165 (Finn J) (Austl.).

When one State submits a Request for Assistance involving Protected Information in the custody of another State, the State receiving the Request for Assistance must verify the validity of the Request for Assistance, the legal basis for compelling access to Protected Information, and the scope and methodology of the Communications Surveillance required are consistent with the publicly available Formal International Channel, international law, and this Implementation Guide. Judicial Authorities should review the Request for Assistance and must give approval prior to initiating any Search or transmittal for or of Protected Information. The requesting State should certify and demonstrate that it has acted in accordance with their substantive responsibilities under the domestic and international law and followed all domestic legal processes.

3. Emergency procedures

In Emergency Circumstances, a Request for Assistance for Protected Information should be initiated under the guidelines of the applicable Formal International Channel. The Request for Assistance for Protected Information should be made through (1) an administrative request or (2) a provisional order from a Judicial Authority.

Relevant principle(s): Legality, Competent Judicial Authority, Due Process, and Safeguards Against Illegitimate Access

A Government Agent may make a Request for Assistance for Protected Information via a Formal International Channel under Emergency Circumstances by seeking an administrative application or a provisional order from a Judicial Authority. In either instance, the Government Agent must certify that there are reasonable grounds to believe Communications Surveillance will ultimately be approved by a Judicial Authority of the State receiving the request. As soon as possible after the Request for Assistance is made under Emergency Circumstances, the State seeking the Protected Information should submit a follow-up authorization Request under non-emergency protocols through the Formal International Channel. If a Government Agent or Judicial Authority of either the seeking or receiving State determines at any time that the Emergency Circumstance no longer exists, the parties must return to non-emergency protocols.[69]

[69] Similar emergency protocols exist for international asset recovery; see Jean-Pierre Brun et al., *Asset Recovery Handbook: A Guide for Practitioners*, The World Bank and United Nations Office on Drugs and Crime, 135-6, 2011, *available at* http://www.unodc.org/documents/corruption/Publications/StAR/StAR_Publication_-_Asset_Recovery_Handb ook.pdf.

4. Safeguards and grounds for refusal

All agreements for the international transfer of Protected Information must include human rights safeguards. States should only initiate and maintain full cooperation relationships with States whose justice systems adequately protect human rights. States should ensure that any request for User Data complies with international law and policies and human rights.

Relevant principle(s): Safeguards for International Communication

All Formal International Channels must include human rights safeguards. The agreements should require the refusal of any requests for assistance that raise human rights concerns, such as a serious risk of a user being subjected to torture or the death penalty on the basis of the requested Protected Information. Protected Information should only be provided where the acts or omissions constituting the offence would have constituted an offence if they had occurred in the requested State (i.e., dual criminality).

Before entering into an agreement to cooperate with one another, States should analyze each other's criminal justice systems to determine whether they adequately protect human rights. States should periodically review these assessments to ensure other States are complying with human rights standards.

Implementing example:
Article 4 of the UN Model Treaty on Mutual Assistance in Criminal Matters contains grounds for refusal in circumstances such as where the request relates to a political offence, raises double jeopardy concerns or involves persecution on the basis of race, sex, religion, nationality, ethnic origin, or political opinions. However, these are not mandatory protections.[70]

[70] UN General Assembly, *Model Treaty on Mutual Assistance in Criminal Matters : resolution l adopted by the General Assembly.*, April 3, 1991, A/RES/45/117, *available at*: http://www.refworld.org/docid/3b00f21e1c.html.

IV. Appendices

Appendix A: The International Principles on the Application of Human Rights to Communications Surveillance

LEGALITY

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

LEGITIMATE AIM

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

NECESSITY

Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State.

ADEQUACY

Any instance of Communications Surveillance authorized by law must be appropriate to fulfill the specific Legitimate Aim identified.

PROPORTIONALITY

Communications Surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests. This requires a State, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

1. There is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out, and;
2. There is a high degree of probability that evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought, and;
3. Other less invasive techniques have been exhausted or would be futile, such that the technique used is the least invasive option, and;
4. Information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged, and;
5. Any excess information collected will not be retained, but instead will be promptly destroyed or returned, and;
6. Information will be accessed only by the specified authority and used only for the purpose and duration for which authorization was given, and;
7. That the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

COMPETENT JUDICIAL AUTHORITY

Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

1. Separate and independent from the authorities conducting Communications Surveillance;
2. Conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights; and
3. Have adequate resources in exercising the functions assigned to them.

DUE PROCESS

Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law, except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorization must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorization.

USER NOTIFICATION

Those whose communications are being surveilled should be notified of a decision authorizing Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorization. Delay in notification is only justified in the following circumstances:

1. Notification would seriously jeopardize the purpose for which the Communications Surveillance is authorized, or there is an imminent risk of danger to human life, and;
2. Authorization to delay notification is granted by a Competent Judicial Authority, and
3. The User affected is notified as soon as the risk is lifted as determined by a Competent Judicial Authority.

The obligation to give notice rests with the State, but communications service providers should be free to notify individuals of the Communications Surveillance, voluntarily or upon request.

TRANSPARENCY

States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities. They should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting Communications Surveillance. States should not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with State requests for Communications Surveillance, adhere to those procedures, and publish records of State requests for Communications Surveillance.

PUBLIC OVERSIGHT

States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance. Oversight mechanisms should have the authority: to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been comprehensively and accurately publishing information about the use and scope of Communications Surveillance techniques and powers in accordance with its Transparency obligations; to publish periodic reports and other

information relevant to Communications Surveillance; and to make public determinations as to the lawfulness of those actions, including the extent to which they comply with these Principles. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

INTEGRITY OF COMMUNICATIONS AND SYSTEMS

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

SAFEGUARDS FOR INTERNATIONAL COOPERATION

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

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS AND RIGHT TO EFFECTIVE REMEDY

States should enact legislation criminalizing illegal Communications Surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence or otherwise not considered in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through Communications Surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected.

Appendix B: Implementation Guide Checklist

Note: capitalized words below are defined terms developed for this guide (see Terminology in this Guide, Section II).

I. The Request

- Based on publicly available, discernable law;
- Applicable to only a single Target;
- Narrowly tailored to minimize the impact on Protected Information;
- Written and signed by a Government Agent and Approved by an independent and competent Judicial Authority, who evaluates the Request based on both the content and the sufficiency;
- Describes the Account, Device, or Repository subject to Communications Surveillance, the Necessary Information sought, any Protected Information that may be incidentally accessed, the methodology to be used, and the specific timetable for the Communications Surveillance;
- Establishes that the Necessary Information sought is contained in the Account, Device, or Repository identified for Communications Surveillance;
- Demonstrates a sufficient nexus between the Account, Device, or Repository to be subject to Communications Surveillance and the Necessary Information sought;
- Where emergency procedures are used, a formal application is filed within 24-72 hours after the initiation of the Search.

II. The Court Order

- Issued and signed by an impartial, competent, and independent Judicial Authority;
- Pursuant to public and transparent proceedings;
- Based on credible, lawfully acquired information;
- In writing, identifying all underlying legal authorities and with the Request attached;
- Describes the full scope of the authorization, including the Accounts, Devices, or Repositories to be subject to Communications Surveillance, as well as the scope, timeline, and methodology for the Communications Surveillance;
- Narrowed to ensure minimal incidental access to Protected Information;
- Limits the retention time for all Protected Information to a reasonable time, not to outlast the resolution of the Legitimate Aim of the Communications Surveillance;
- Includes a written opinion explaining the issues and the rationale for the decision in all cases of novel or unique factual or legal issues;
- Requires reporting on all Protected Information acquired during the Search,

including collection, access, retention, and eventual destruction; and
- In the case of emergency procedures, limits the authorization to the time reasonably necessary for the Government Agent to complete a proper Request.

III. The Provider's Response

- Responds only to Requests in writing and including the identify of the Government Agent making the Request as well as a clear description of the scope, duration, and methodology of the Communications Surveillance to be conducted;
- Formally challenges all Requests outside the scope of domestic or international laws that should be formally challenged;
- Unless legally prohibited from doing so, requires notification to the user of the Request;
- Limits the Search precisely to the bounds of the Request and provides no more information than the most narrow construction requires; and
- Provides regular transparency reports to document all Requests.

IV. Execution of the Court Order

- Notifies the Target of the Court Order and provides an adequate opportunity to challenge the validity of the Search unless there is a demonstration that a delay is necessary;
- Regularly reports back to the Judicial Authority all of the Protected Information acquired during the Search;
- Segregates relevant information, promptly discards irrelevant information, and destroys evidence at the conclusion of the case or when it is no longer required;
- Respects Formal International Channels for any Request to or from an international jurisdiction;
- Prevents the use of any Protected Information that was not legally obtained from being used in any judicial proceeding or as the basis for further investigtations;
- Reimburses all costs to Providers within a reasonable time; and
- Compiled within regularly published transparency reports on the usage of Communications Surveillance authorities and practices.

Appendix C: [Case Study 1] Twitter Parody Case in Chile

In 2011, a blogger named Rodrigo Ferrari created a Twitter account with the username "@losluksic." The account included a picture of three members of the Luksic family, one of the wealthiest families in Chile.[71] Behind the picture of the three relatives were images of money bills. The account tweeted comments like "tenemos cualquier plata" ("we are so loaded").

One of the family members, Mr. Andronico Luksic, filed a criminal complaint for the creation of this account and for two other accounts ("@andronico_luksic" and "@luksic_andronico"). The complaints were based on a misdemeanor, "usurpaci6n de nombre" ("name usurpation") whose single element is the appropriation of another person's identity.

Twitter is outside Chilean jurisdiction because its headquarters and servers are in California. Therefore, the prosecutor from the Chilean Public Ministry filed a request to the U.S. government under the Inter-American Treaty on Mutual Assistance in Criminal Matters seeking the IP addresses of the Twitter accounts and the identity and contact information of their owners. The prosecutor skipped the mandatory step under the Chilean Criminal Procedure Code of seeking judicial authorization.[72]

In response to the MLAT request, Twitter provided the IP addresses to the prosecutor. The prosecutor then directly asked the Chilean mobile phone provider, V.T.R. Telecomunicaciones, for the ISP account information linked to the IP addresses. V.T.R. Telecomunicaciones provided Rodrigo Ferrari's information. Although Mr. Ferrari is only the owner of the "@loslukic" account, the prosecutor charged him for creating all three accounts based on deficient and misconstrued police reports.

On April 1, 2013, a judge in Chile dismissed the charges against Mr. Ferrari ruling that it was clear that the "@losluksic" account was a parody account, and punishing him would infringe the fundamental right to freedom of expression.

Lessons Learned

The Chilean Government

- The Chilean prosecutor should have sought judicial authorization before sending a request to the U.S. government, and again before sending a Search request to V.T.R. Telecomunicaciones (due process).

- The Chilean Public Ministry should have confirmed that all requirements under Chilean law had been met before sending the MLAT request to the U.S.. This

[71]Forbes, Worlds Richest Families: Andronico Luksic & family (2005), *available at* http://www.forbes.com/static/bill2005/LIR0CJD.html.
[72] Unlike U.S. law, which does not require a court order for subscriber information, Chilean law dictates that any Search for information must be approved by a Judicial Authority.

includes judicial authorization, as well as the broader issue of whether pursuing prosecution under this law is appropriate (due process, legality, proportionality).
- Since there were three accounts involved, the Chilean Prosecutor and the Chilean Public Ministry should have submitted separate search requests for each account (proportionality).

The U.S. Government

- The U.S. government should have required that the request satisfied dual criminality, particularly given the implications for freedom of speech (legality).
- The U.S. Department of Justice should have sought judicial authorization from a U.S. court to access the user's IP address, which is Protected Information (competent Judicial Authority).

Twitter

- Twitter should have ensured that the request was specific and that the Search was authorized by pertinent legal procedures (necessity, adequacy, legality, and proportionality).

V.T.R. Telecomunicaciones

- V.T.R. Telecomunicaciones should have refused to provide the information sought by Chilean prosecutors until served with a valid and properly issued court order (due process).

The Chilean Judge

- The judge correctly dropped the complaint against Mr. Ferrari, recognizing the account as a parody, which constitutes protected expression.[73] The judge should also have granted indemnification of legal costs and damages (safeguards against illegitimate access).
- The judge should have made sure that the Chilean prosecutor properly discarded all the information that relates to Mr. Ferrari (safeguards against illegitimate access).
- Civil, criminal, or disciplinary sanctions against the prosecutor and Public Ministry should be considered.

[73] Renata Avila, *#FreeRod: Preliminary Victory in Chilean Twitter Parody Case*, GlobalVoices Advocacy, (April 24, 2013, 17:48 GMT), http://advocacy.globalvoicesonline.org/2013/04/21/freerod-preliminary-victory-twitter-parody-case/.

APPENDIX D: [Case Study 2] An Overreaching Subpoena — Surveillance of the Associated Press' Records

In May 2013, the U.S. Department of Justice sent a letter to the Associated Press ("AP") notifying them of a two-month Search of call records of AP personnel from 2012. This covered approximately 20 work and personal phone numbers from 40 AP reporters and editors in three different states. Reports indicate that the Department of Justice (DOJ) was trying to uncover the source of information that the AP published a year before on a foiled terror plot.

In its letter to the AP, the DOJ stated that it had issued subpoenas to conduct the Search (an administrative process, not requiring the approval of a judge). The New York Times revealed that telecommunications carriers (including Verizon Wireless) handed out the information to the DOJ without questioning whether they should make their customers aware of the Search.[74]

Such conduct not only creates a chilling effect on the freedom of expression of journalists, but it also raises fears for human rights defenders, whistleblowers, and the general public. The widespread collection of information also violates the due process rights of the journalists, since their privacy was interfered with proper oversight or limitations.

The U.S. government has insisted that federal laws allow it to do non-content Search through a subpoena. This case demonstrates that a lot can be revealed simply by searching a user's numbers, who that user calls, the length of calls, and the location where the calls were made. This calls for a revision of U.S. federal laws to ensure that a court warrant will be used every time a user's identify, associations, communications, and locations can be discerned.

Lessons Learned

The U.S. Attorney General's Office

- The Attorney General should have sought authorization for the Searches from an impartial, competent, and independent Judicial Authority (competent Judicial Authority).

- The Request should have been narrowed in time and scope. Call records of 20 numbers from three different states involving more than 40 individuals for two months is an overbroad Search (proportionality, adequacy, and necessity).

- The Search should have been limited to one court order per telephone number.
- The Request should have demonstrated that other less burdensome techniques were exhausted, that this Request was made pursuant to a Legitimate Aim, that

[74] Charlie Savage and Scott Shane, *Justice Dept. Defends Seizure of Phone Records, New York Times*, May 13, 2013, *available at* http://www.nytimes.com/2013/05/15/us/politics/attorney-general-defends-seizure-of-journalists-phone-record s.html?pagewanted=1&_r=2&hp..

there was a fair level of probability that the information would be found, and that this type of Search was absolutely necessary to acquire the sought information.
- The government should have notified the AP (and other affected users) that their accounts were accessed as soon as possible (after any of the risks indicated in the section on notification exceptions had abated).

The Telecommunications Carriers (including Verizon Wireless)

- The telecommunications carriers should have challenged the overly broad Request and interpreted it as narrowly as possible.
- Unless the telecommunications carrier is prohibited from doing so, it should notify its clients promptly. While the government had the primary responsibility to notify the Associated Press, Verizon Wireless should have at least inquired whether it could notify the journalists.