



Derek Moore
Office of Policy Planning
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Via electronic filing

December 20, 2018

Re: 21st Century Hearings Consumer Privacy Background and Questions for Comment
(Docket ID: FTC-2018-0098-0003)

Dear Mr. Moore,

Thank you for the opportunity to submit pre-hearing comments to the Federal Trade Commission (FTC) ahead of the next session of the series of Hearings on Competition and Consumer Protection in the 21st Century focussing on Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matter (Topic 5) which will be held on February 12-13, 2019.

We welcome the open and comprehensive process initiated by the FTC through these hearings. Below we provide general comments on privacy protections in the United States and on the role of the Commission in protecting privacy as well as specific feedback to questions posed by the FTC.

About Access Now

Access Now is an international organization that defends and extends the digital rights of users at risk around the world.¹ By combining innovative policy, user engagement and direct technical support, we fight for a free and open internet that fosters human rights. As part of our mission, we operate a global digital security helpline for users at risk to mitigate specific threats they face. Additionally, we work directly with lawmakers at national and international fora to ensure policy decisions are focused on the rights and interests of users, particularly those most at risk.

We defend privacy and data protection globally. For example, Access Now provided comments on the development and implementation of data protection and privacy rules in the Brazilian Marco Civil,² the African Union Convention on Cyber Security and Personal Data Protection,³ the Federal

¹ <https://www.accessnow.org/>

² <https://www.accessnow.org/brazil-must-protect-marco-civil-regulatory-decree/>

³ <https://www.accessnow.org/african-union-adopts-framework-on-cyber-security-and-data-protection/>

Communications Commission (FCC) broadband consumer privacy rules,⁴ India's Expert Committee on data protection,⁵ and in the EU, we have been involved in the data protection reform process since the tabling of the General Data Protection Regulation (GDPR) by the EU Commission in January 2012.⁶

Most recently, Access Now provided comments to the National Telecommunications and Information Administration (NTIA) on Developing the Administration's Approach to Consumer Privacy and to the National Institute of Standards and Technology (NIST) on Developing a Privacy Framework.⁷ While these processes are happening in parallel to the FTC's, we hope to see these efforts become complementary and mutually-reinforcing. For ease of reference, we attach the full text of our input to the NTIA and NIST as Appendices A and B, respectively.

In addition, as Appendix C we are attaching "Creating a Data Protection Framework: a Do's and Don'ts Guide for Lawmakers," a detailed Access Now report about the passage and implementation of the GDPR in the EU. On the basis of our analysis, we proposed a framework for a federal statute on the protection of personal data, which we detail in our submission below.⁸ We believe the resources on international standards and practices will be useful for the FTC's hearings.

General Comments

Protecting personal data, or personally identifiable information (PII), means establishing clear rules for any entity, whether public or private, that processes such information. Data protection laws have been in place in many countries around the world for more than 40 years, but they are increasingly important as the sharing, collection, and use of data has skyrocketed. The first data protection law was passed in 1970 by the German federal state of Hesse.⁹ A few years later, the U.S. developed the "fair information practices," which influenced the development of data protection laws around the world.¹⁰ Unfortunately, the U.S. has yet to establish a comprehensive legal framework for data protection at the federal level. Instead, the U.S. has implemented a sector-specific approach to protecting privacy and data protection, which has been of limited value in mitigation or enforcement of the recent large-scale data protection incidents.¹¹ The impact of a U.S. law on privacy, where many leading technology companies are headquartered, would be significant. It is time for the U.S. to pass a comprehensive law protecting user privacy.

In the EU, data protection is a fundamental right intrinsic to every individual and protected at the constitutional level.¹² All actors in society, public or private, must observe and respect data protection. To that end, rules have been developed through EU secondary legislation with the

⁴ https://www.accessnow.org/cms/assets/uploads/2016/05/NPRM-PrivacyofBroadbandCustomers-_-Access-Now.pdf

⁵

https://www.accessnow.org/cms/assets/uploads/2018/01/Access-Now_Responses-to-White-Paper-on-Data-Protection_January-31-2018.pdf

⁶ <https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf>

⁷ <https://www.accessnow.org/cms/assets/uploads/2018/11/NTIA-Consumer-Privacy-Comments.pdf>;

<https://www.accessnow.org/cms/assets/uploads/2018/12/NIST-Privacy-Engineering-Comments-Access-Now.pdf>

⁸ <https://www.accessnow.org/data-protection-in-the-united-states-heres-what-we-need-to-protect-the-users/>

⁹ Hessische Datenschutzgesetz, original version dated from 7 October 1970. (GVBl. I S. 625)

¹⁰ https://epic.org/privacy/consumer/code_fair_info.html

¹¹ <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/>

¹² https://edps.europa.eu/data-protection/data-protection_en

GDPR and the Police Directive comprising the current legal framework. The GDPR has influenced data protection laws globally. Other countries, including Tunisia, Brazil, Japan, Argentina, and Jamaica have adopted, are updating, or are nearing passage of their own laws.¹³ Similarly, an expert committee in India is deliberating with the government on a data protection and privacy regime that would extend protections for hundreds of millions of internet users.¹⁴ The U.S. is notably missing from the list of countries that have established or are nearing the establishment of a national framework. Once a pioneer in the protection of privacy, the U.S. is at risk of becoming an outlier in the failure to adequately protect individuals' information. Nonetheless, the U.S. still has an opportunity to demonstrate global leadership.

The ongoing privacy work by the NTIA, the NIST, and the FTC, as well as legislative opportunities at the federal and state levels provide a chance to bring privacy and personal data protection into the 21st century. To succeed, these processes must provide the opportunity for participation of civil society, academics, and consumer organizations; be transparent; and have goals and outcomes that align.

Responses to request to comments

General Questions

- What are the actual and potential benefits for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these benefits?

Nowadays, an increasingly large number of products, services and applications are offered on the basis of data processing, including collection and use of information. In the tech industry, including search engines, cloud and email providers, and app builders, business models are often based on data processing. The use of data, however, is not limited to tech companies with nearly every sector now processing data. These services can bring users value through simplification and efficiency gains, including for communication, online shopping, food delivery, holiday planning and bookings, and much more. The data-focused economy has led to the creation of new products and services and increased access for communities that otherwise may have been left out.

Data processing can happen in a privacy-friendly manner. A new approach is developing where products and services are created under the principles of data protection and privacy by design.¹⁵ This includes collecting only the information necessary for the delivery of services, implementing appropriate data security practices, providing transparency about the collection and use of data, and granting users rights and control over their data.¹⁶ These principles can be better adopted by search engines, secure cloud providers, messaging applications, online advertising companies, email providers, online shopping, and games. Stronger privacy design benefits users with reduced privacy risks and allows service providers and software developers to enjoy a higher level of trust.

¹³ <https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf>

¹⁴

<https://www.forbes.com/sites/sindhujabalaji/2018/08/03/india-finally-has-a-data-privacy-framework-what-does-it-mean-for-its-billion-dollar-tech-industry/#38cf09a470fe>

¹⁵ https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf

¹⁶ https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf

Industry will continue to develop in a competitive environment that rewards innovative privacy solutions and protects privacy rights.

That said, the concentrations of data and the competitive dynamics of the current data economy pose barriers to fully reaping those benefits. On December 18, the New York Times revealed that Facebook gave tech giants greater access to people's data than it has disclosed to the public and to members of the U.S. Congress. According to the *Times*, through some "special arrangement," Facebook increased its ad revenue while Amazon, Microsoft, Spotify, Netflix and others gained access to massive amounts of private user data, including private messages, without oversight and without people's knowledge or consent.¹⁷ Similarly, the publication of documents by the UK Parliament revealed how Facebook gave preferential access to data to "whitelisted" companies, without users knowledge or consent, and while making access harder for rivals such as Twitter's defunct video app Vine.¹⁸

The permission-less dynamism of the internet, where companies can invest and develop despite risk, must be strongly protected. Yet, network effects and the winner-take-all characteristics of multi-sided platforms operating in the data-focused economy may be limiting the viability of some products and services. The concentration of personal data can be a barrier to start-ups that would otherwise bring innovation to markets.

- What are the actual and potential risks for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these risks?

A recent analysis by NTIA from data collected from 41,000 households with at least east one internet user found that "Americans are increasingly concerned about online security and privacy at a time when data breaches, cybersecurity incidents, and controversies over the privacy of online services have become more prominent."¹⁹ Indeed, as our societies become more connected and the amount of personal data disclosed, shared, and available online continues to grow, risks and vulnerabilities also increase.

According to the NTIA analysis, these concerns have driven some users to limit their online activity, including communications and commercial transactions. For instance, 45 percent of online households reported that privacy and security stopped them from "buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the internet."²⁰ Since this study, the scope and scale of privacy and security incidents have only increased, affecting billions of users of some of the largest companies in the world such as Facebook and Equifax.

¹⁷ <https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>

¹⁸ <https://www.theguardian.com/technology/2018/dec/05/facebook-documents-uk-parliament-key-facts>

¹⁹

<https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>

S

20

<https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>

S

In response, several agencies and organizations, including the NTIA, have proposed measures aiming at increasing users' trust in entities processing information. Counterintuitively, this framing puts the obligation to act to ensure data privacy on users instead of the processors. The processors must demonstrate they are worthy of receiving and processing user data to earn user trust. To develop that trust, it is the responsibility of companies to respect rights and provide sufficient information in a manner that facilitates users' control and understanding of the scope and purpose of any processing. No amount of trust would have mitigated the harm caused by major privacy and security incidents, and preventing future breaches requires affirmative efforts from and changes in the behavior of companies.

People produce digital footprints at an alarming rate. Almost everything we do online or off can be—and often is—tracked by digital platforms. Already by 2012 Facebook was collecting about 180 petabytes of data per year.²¹ A recent investigation from the New York Times revealed how companies can receive precise location data from apps to track users, often without their knowledge.²² Several businesses claim to track up to 200 million mobile devices in the United States alone.²³ This data can reveal people's travels in startlingly detail, down to a few yards, and thousands of times a day. Location tracking can be processed along with other personal information. Google knows not only users' search histories on their platforms, but can also track users across websites and devices. Google can also know apps users installed on the Android operating system, and their location.²⁴

This growth in large scale collection, retention, transfer, and analysis of personal data places everyone's privacy at risk. The recent news of Cambridge Analytica's access to the Facebook data of 50 million users, and retention of that data despite requests by Facebook to delete it, demonstrates some of the potential harms from business practices based on wide-scale collection of user information.²⁵ Cambridge Analytica was a company headquartered in the United Kingdom that has been noted for its role in interfering and manipulating elections globally.²⁶ The latest scandal highlights the company's intervention in United States elections, where Cambridge Analytica's activities were bolstered by targeted advertising made possible only because of all the data Facebook collects and Cambridge Analytica's access to this data.²⁷

Digital platforms whose business model is based on data harvesting do pose threats to privacy alone. Other consumer facing companies, third party data brokers, and government agencies develop comprehensive profiles with information that may be sensitive, including names, addresses, phone numbers, buying habits, personal interests, ethnic identities, political affiliations,

²¹ For reference, one petabyte is the equivalent of 20 million 4-drawer filing cabinets filled with text.

²² <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>

²³ <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>

²⁴ <https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy>

²⁵

<https://www.accessnow.org/its-not-a-bug-its-a-feature-how-cambridge-analytica-demonstrates-the-desperate-need-for-data-protection/>

²⁶ <https://www.bbc.com/news/world-43476762>

²⁷ <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>

marital status, credit card details, and numerous other data points.²⁸ Enough information is often collected that supposedly anonymous information can be used to re-identify the data subject.²⁹

This means that privacy protections for the internet age must extend far beyond consumers. Many of the tools and services used by people today are not goods in the traditional sense—people do not pay money to use them, and they do not necessarily receive a tangible product in exchange. Instead, entities monetize users' personal information. Such use of data often happens with or without users' knowledge and often with the user unable to use the service otherwise. The privacy implications are heightened when the user's data is the sole product.

For example, social media users are probably not “consumers” within the traditional definition as they are not paying money for the service. Nonetheless, these services based on expansive collection and processing of personal information should undoubtedly be subject to data privacy rules or regulations. Entities like data brokers can passively collect information from people with whom they may never interact with at all.³⁰ In fact, these companies may maintain and sell comprehensive data profiles with users who do not even know the company exists.³¹

Taken in aggregate, millions of data points implicate privacy and other rights at the societal level. For example, data protection can help reduce the risk of that personal information will be used to manipulate how we associate and engage in democracy. For these reasons, focusing solely on “consumers,” under a traditional understanding of the term, would fail to capture the full range of privacy risks. Instead, the focus should be on the risks and rights of all people in the U.S.

- The use of “big data” in automated decision making has generated considerable discussion among privacy stakeholders. Do risks of information collection, sharing, aggregation, and use include risks related to potential biases in algorithms? Do they include risks related to use of information in risk scoring, differential pricing, and other individualized marketing practices? Should consideration of such risks depend on the accuracy of the underlying predictions? Do such risks differ when data is being collected and analyzed by a computer rather than a human?

Automated decision making refers to the processing of data to derive or evaluate information about a user or a group of user, in particular to analyze or predict attributes, interests and/or behavior.³² Techniques such as profiling, often used in automated decision making, create heightened risks to users' privacy as sensitive information can be predicted from the aggregation of data. Profiles are used to make or inform consequential decisions, from credit scoring, to health benefits, hiring processes, border controls and national security.³³ Automated decision making processes and

²⁸ <https://newrepublic.com/article/115041/what-big-data-does-and-doesnt-know-about-me>

²⁹

<https://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/>; <https://www.nytimes.com/2006/08/09/technology/09aol.html>

³⁰ https://motherboard.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection

³¹ https://motherboard.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection

³²

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/>

³³ <https://www.theguardian.com/science/2016/sep/01/how-algorithms-rule-our-working-lives>

profiles are generally opaque, may be inaccurate, and are not always done at the consent of the data subject.³⁴

In the EU, the GDPR provides users with an extended right to object, which includes the right for users to not be subject to a decision based solely on automated processing, including profiling.³⁵ In the U.S. approach, including under Graham-Leach-Bliley Act, users are provided the right to opt-out of sharing of their profiles with certain third parties, but not the right to object to automated decision making and profiling as a whole.³⁶

The ability to opt-out is a flawed mechanism for the use of automated decision making. Opt-out mechanisms are typically cumbersome to use and offer little notice or explanation on the nature of the use, and worse, can obfuscate methods and purposes. A sectoral requirement for credit rating exists in the U.S. serves as a useful example. The Fair Credit Reporting Act (FCRA) safeguards users against credit rating abuses by allowing users to contest mistakes made in their credit ratings.³⁷ The information fed into credit scores can come from a number of sources and are liable for misuse.³⁸ These frameworks, however, offer only limited ability to opt-out of certain practices such as the sharing of their credit rating with third parties or “pre-screening” of unsolicited offers of credit. A credit score plays an essential role in the process of getting a loan or renting an apartment.³⁹

Beyond the risks for privacy, data protection and security, automated processes can facilitate intentional or inadvertent discrimination against certain individuals or groups of people.⁴⁰ Based on automation, individuals can be rejected from job opportunities, denied schooling or health benefits, or their demographics can determine their access to justice.⁴¹ Existing patterns of structural discrimination may be reproduced and aggravated by the use of automated processes, for example, from using non-representative or biased datasets.⁴² Ensuring that a human is involved in the decision making process can help bring accountability and mitigate the risks of discrimination and biases.

- Should privacy protections depend on the sensitivity of data? If so, what data is sensitive and why? What data is not sensitive and why not?

All personal data, sensitive or not, should be protected, but the heightened harms from misuse of sensitive information means users should have greater control. In various jurisdictions, sensitive data encompasses a wide range of personal information such as ethnic or racial origin, religion or

³⁴

<https://www.theguardian.com/technology/2017/jan/27/ai-artificial-intelligence-watchdog-needed-to-prevent-discriminatory-automated-decisions>

³⁵ See Article 21 of the GDPR, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>

³⁶ See the Gramm-Leach-Bliley Act,

<https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

³⁷ <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act>;

<https://www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf>

³⁸ <https://www.epic.org/privacy/fcra/>

³⁹ https://www.huffingtonpost.com/nerdwallet/no-credit-vs-bad-credit-k_b_11318764.html

⁴⁰ https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf

⁴¹ <https://www.theguardian.com/science/2016/sep/01/how-algorithms-rule-our-working-lives>

⁴² <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

other beliefs, memberships, physical and mental health including genetic and biometric data, information about personal life and sexuality, or criminal or civil offences.⁴³ Given the importance, the collection and processing of sensitive personal data should only be permitted if individuals give their explicit and informed consent and are granted the right to withdraw that consent.

- Should privacy protection depend on, or allow for, consumer variation in privacy preferences? Why or why not? What are the appropriate trade offs to consider? If desired, how should this flexibility be implemented?

Article 12 of Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) recognize the right to privacy as a fundamental right and states that this right should not be subjected to arbitrary interference.⁴⁴ The U.S. is a party to both instruments. Pursuant to these instruments and other elements of international law, the UN Guiding Principles on Business & Human Rights, elaborating the UN Ruggie ‘Protect, Respect, Remedy’ Framework (“Ruggie Principles”), establishes that all states and companies have the responsibility to understand the impact of their products and services on human rights, locally and globally, including the right to privacy. Companies should take measures to prevent and mitigate any adverse impacts they cause or contribute to, including through conducting human rights due diligence, consulting external stakeholders from affected communities, and developing policies that respect rights and address risks posed to human rights as a matter of priority. The third pillar of the Ruggie Principles states that companies and governments should jointly provide affected persons with meaningful access to remedy for any business-related harms.⁴⁵ To protect privacy as a human right globally, it shall be protected at all time and for all users, regardless of steps taken to demonstrate preference.

In the same way the U.S. Constitution and existing privacy laws provide a baseline privacy protection, so too should any future privacy laws. The recent U.S. Supreme Court decision in *U.S. v. Carpenter* demonstrated the Court’s adaption to user attitudes on privacy by extending the Fourth Amendment warrant requirement for law enforcement access to wide-scale collection of cell phone location information. The Court determined that a person holds “a legitimate expectation of privacy in the record of his physical movements as captured through cell phone location information.”⁴⁶ In the same way the Court extended a baseline privacy protection for cell phone location information, so too should any data protection law establish baseline protection outside of any demonstrated preference by the user.

- Market-based injuries can be objectively measured—for example, credit card fraud and medical identity theft often impact consumers’ finances in a directly measurable way. Alternatively, a “non-market” injury, such as the embarrassment that comes from a breach of sensitive health information, cannot be objectively measured because there is no functioning market for it. Many significant privacy violations involve both market and non-market actors, sources, and harms. Should the Commission’s privacy enforcement and policy work be limited to market-based harms? Why or why not?

⁴³ <https://www.linkedin.com/pulse/20140731172016-2259773-what-is-sensitive-data-different-definitions-in-privacy-law>

⁴⁴ <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf>;

<https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>

⁴⁵ http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

⁴⁶ https://www.supremecourt.gov/opinions/17pdf/16-402_new_o75q.pdf

NTIA's analysis of recent data demonstrated that many Americans have refrained from engaging in important online activities, including economic and civic ones, due to privacy and security concerns.⁴⁷ The decrease in user trust in the way online services handle personal information is resulting in falling market values for tech companies.⁴⁸

Beyond the objectively measurable economic and financial costs linked to the lack of privacy for the industry or users, it is important to note that there is no model we are currently aware of to assess the comprehensive cost of individual privacy risks, either on average or specific to a person. Accordingly, more research is necessary in order to determine metrics for evaluating impact. Investment should be made in this research on harms that are not intrinsically financial. Instead, it must also include emotional, psychological, physiological, human rights, and other impacts that individuals may face on account of an event that impacts their privacy. It should also include a probe of possibilities for individual and collective remedies, including the options people may have to respond to or mitigate those impacts.

Finally, when it comes to the assessment, it should also be noted that risk is often wrongly only considered in relation to the volume of data at risk. Entities processing large amount of data shall indeed have stringent security and privacy obligations. However, this does not necessarily mean small data sets or data processing activities are without significant risks. Beyond volume, risks must also take into account the type of data, including particularly sensitive data types such as health and biometric, and the scope and sensitivity of the inferences that can be drawn.

- In general, privacy interventions could be implemented at many different points in the process of collecting, processing, and using data. For example, certain collections could be banned, certain uses could be opt-in only, or certain types of processing could trigger disclosure requirements. Where should interventions be focused? What interventions are appropriate?

Privacy interventions should focus on providing users with more information and control over the use of his or her data. Examples of such interventions include specific protection and obligation regarding the processing of sensitive data described above. In addition, personal data processing should only happen in accordance with specific bases enumerated in law. These may include for example, meaningful opt-in consent, execution of a contract, or as otherwise necessary under law. The bases for processing data should be identified by the entity, along with the purpose for which that processing is conducted. Moreover, the amount and category of personal data collected and used shall be limited to what is necessary in relation to the defined purpose. Discriminatory or overly vague description should not be considered acceptable purposes.

Finally, users should have a series of enforceable rights and receive an explanation from entities processing their personal data, whether the processor collected the data directly or received it through third parties. All the information provided to the user should be provided in concise,

⁴⁷

<https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>

⁴⁸ <https://medium.com/ipg-media-lab/how-tech-companies-are-failing-the-trust-test-1f1057de9317>

intelligible, and easily accessible form, using clear and plain language. This information should include details about data being processed, the purpose of this processing, and the length of storage, if applicable. The entities should provide their contact details and an email address to allow users to contact them in case they seek more information.

- Should policymakers and other stakeholders attempt to improve accountability for privacy issues within organizations? Why or why not? If so, how? Should privacy risk assessments be mandated for certain companies? Should minimum standards in privacy protections be required?
- How can firms that interface directly with consumers foster accountability of third parties to whom they transfer consumer data?

Privacy is often better protected with binding obligations for entities processing data, enforceable rights for users, and access to remedy. Building on our global data protection work, we have created recommendations for a comprehensive legislative approach to privacy and data protection. These are the elements necessary to fully protect people, in the U.S. and elsewhere, in our increasingly connected world.

First, a comprehensive set of data protection laws should apply equally to any entity that collects, uses, or manipulates information about people, whether public or private. It should not preempt or prevent the creation of any stronger protections that are already written into federal law or exist at the state level. It should also be forward looking, contemplating the wealth of information that will be available through the Internet of Things and other connected devices. And it should support the growth of business models that are not built on the collection and exploitation of massive amounts of sensitive data.

To enforce the law, an independent data protection commission should have extensive authority and resources to monitor implementation, conduct investigations, and sanction entities. The rights afforded to users should include the following:

- **Right to access** which enables users to obtain information from entities 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.
- **Right to object** which 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 valid contract. This right to object should apply to automated decision-making mechanisms, including profiling, as users should have the right not to be subjected to the use of these techniques.
- **Right to erasure** which allows users to request the deletion of all personal data related to them, including profiles that may have been created, when they leave a service or application.
- **Right to rectification** which allows users to request the modification of inaccurate information about them.

- **Right to information** which 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.
- **Right to explanation** which empowers users to obtain information about the logic involved in any automated 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.
- **Right to portability** which 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.

Finally, the legislation should obligate all entities processing data to limit processing to specific bases enumerated by law, including meaningful opt-in consent, execution of a contract, or as otherwise necessary under law. Entities should minimize data by only collecting the data necessary for the identified purposes. Affirmative obligations shall be created for the processor to timely notify users when, and to whom, data are transferred, eliminating the shadow internet industries built around user data. The law should create a blanket public data breach notification requirement, with individualized notice in the case of potential harm, including emotional harm. It should prohibit the use of algorithms to arbitrarily discriminate, including against marginalized communities and communities of color, and prevent the use of mandatory arbitration clauses for users.

- What should the role of the Commission be in the privacy area? What would define successful Commission intervention? How can the Commission measure success?
- What are the tradeoffs between ex ante regulatory and ex post enforcement approaches to privacy protection? (originally from following section on Legal Frameworks)

The current authority and resources given to the FTC are insufficient to effectively protect users' privacy. The FTC has limited jurisdiction without authority over federal; state; or local agencies, banks and insurance companies, and other entities regulated by other agencies.⁴⁹ All these entities conduct data processing that impact privacy. The FTC cannot comprehensively guarantee privacy rights unless jurisdiction is extended to any entity that processes data.

The FTC is already underfunded and has faced complications in attempting to enforce privacy protections.⁵⁰ Where the FTC does investigate, those investigations often lack transparency.⁵¹ Privacy would be better protected with binding legislation providing for obligations for entities processing data, enforceable rights for users, and avenues for remedy. A data protection law should be enforced by an independent commission with extensive powers and resources to make rules, monitor implementation, conduct investigations and enforcement.

Under the current limited scope for privacy enforcement, the FTC has used or attempted to use its powers to protect privacy on several occasions. A number of companies such as Facebook and

⁴⁹ <https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>

⁵⁰ <https://www.publicknowledge.org/news-blog/blogs/the-ftc-must-be-empowered-to-protect-our-privacy>

⁵¹

<https://www.ftc.gov/news-events/press-releases/2017/07/acting-ftc-chairman-ohlhausen-announces-internal-process-reforms>

Google have for instance been placed under a consent agreement for deceiving users.⁵² Although consent orders are an important tool in the FTC's toolkit, they are often not enough to effectively protect users. For example, Facebook signed a consent decree with the FTC in 2011, yet the Cambridge Analytica scandal and the revelations that Facebook entered undisclosed data sharing agreements with device manufacturers and other companies showed the limits of the orders. A privacy audit in 2017, conducted by PricewaterhouseCoopers as part of the 2011 consent decree, failed to reveal all of Facebook's data processing arrangements with its partners.⁵³

What is more, the FTC's authority to regulate the data security practices of private companies was recently challenged in the *LabMD v. FTC case*.⁵⁴ The Court ruled an FTC order requiring LabMD to implement certain data security reforms was unenforceable due to vagueness. In doing so, the Court may have limited the Commission's ability to enforce broad remedial orders outside legislative authority and impacted many of the FTC's consent orders—even those not having to do with data security. If the FTC is mandated to act as the primary regulator for privacy and data protections and the enforcement of a comprehensive legislation on users' privacy, it must be given significantly greater resources and authority to carry out its extended mission.

Questions About Legal Frameworks

- What are existing and emerging legal frameworks for privacy protection? What are the benefits and drawbacks of each framework?

European Union

The EU's GDPR is perhaps the most known data protection legislation around the world. Access Now has worked extensively for the passage and on the implementation of the GDPR. We have produced a guide for the development of data protection frameworks based on our experience (see Appendix C). The guide provides 15 concrete recommendations to lawmakers based on 10 positive developments and five areas for improvement with regards to the GDPR. The GDPR, which entered into application on 25 May 2018, is a comprehensive legislation establishing binding obligations for entities processing data, enforceable rights for users and laying down mechanisms for enforcement and remedy. After years of unprecedented lobbying against regulation during the negotiation of the GDPR, the U.S. tech industry performed a u-turn over the legislation and now supports its objectives as shown by recent comments from Apple, Google, Microsoft and, Facebook CEOs and top executives.⁵⁵ While the road toward compliance and data protection by design is still far for a number of these companies, the race to the top for the protection of personal information has started.

⁵²

<https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>;

<https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz>

⁵³ <https://www.epic.org/foia/ftc/facebook/EPIC-18-03-20-FTC-FOIA-20180418-FB-Assessment-2017.pdf>

⁵⁴ <https://www.bgdlegal.com/blog/labmd-and-the-future-of-ftc-data>

⁵⁵

<https://corporateeurope.org/lobbycracy/2013/02/crowdsourced-lobby-expos-shows-internet-giants-have-footprints-our-data-privacy>; <https://www.youtube.com/watch?v=zlniYSkAWo0>; <https://www.youtube.com/watch?v=6ValJMOpt7s>; <https://www.bbc.com/news/technology-45963935>

India

In India, on July 2018, a committee of ten data protection experts published a 176-page report and a draft Personal Data Protection Bill (“Draft Bill”).⁵⁶ The Draft Bill draws inspiration in many instances from the GDPR and the UK Data Protection Act.

Nevertheless, in its current state, the Draft Bill has many hits and misses. Access Now has published a full analysis of the Draft Bill and provided recommendations to the committee of experts to help improve the proposal.⁵⁷ In our analysis, we found that the provisions of the Draft Bill defining the scope of application of the law, along with data security measures proposed for entities, seem to be strong. While the Draft Bill proposes to codify multiple important users’ rights, the right to access and rectify data are limited in scope, and certain key rights such as right to object and the right to explanation are not provided. Most concerning is the proposal for data localisation found in the Draft Bill, given that such measure creates privacy risks for users and negates the importance of secured personal data flow for the digital economy.⁵⁸

Finally, the Data Protection Authority, as currently outlined in the Draft Bill, would not be sufficiently independent from the executive or effective in its functioning. India is making important steps toward the protection of privacy and personal data, even if the current Draft Bill is far from perfect. It is essential that the privacy and data protection framework for the next billion users of the internet is informed by global best practices and further improved to provide for a strong user rights-respecting regime.

Tunisia

In Tunisia, a rather comprehensive proposal for data protection and privacy bill has been drafted. Among many measures, the draft bill includes a series of users rights, rules on international data transfers and the use of CCTV, and a quite robust proposal on gradual sanctions in case of privacy and data protection violations.⁵⁹

While debates on this proposed law are slow, the country has already taken a step forward in the protection of personal data by adhering in 2017 to the Council of Europe Convention 108.⁶⁰ 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

⁵⁶

https://www.business-standard.com/article/economy-policy/here-are-the-hits-and-misses-of-india-s-draft-data-protection-bill-118092600142_1.html

⁵⁷

<https://www.accessnow.org/cms/assets/uploads/2018/10/Assessing-India%E2%80%99s-proposed-data-protection-frame-work-oct18.pdf>

⁵⁸ <https://blog.mozilla.org/netpolicy/2018/06/22/data-localization-india/>

⁵⁹ http://www.inpdp.nat.tn/Projet_ARP.pdf

⁶⁰ <https://www.accessnow.org/tunisia-ratifies-convention-108-affirms-commitment-protection-personal-data/>

signature in 1981.⁶¹ It is the first international document on the protection of personal data, and it had a pivotal role in the adoption of the first Europe-wide data protection law in 1995.⁶² Since its adoption, the Convention 108 was ratified by all 47 member countries of the Council of Europe, and Mauritius, Senegal, Uruguay, Tunisia, Cabo Verde and, most recently, by Mexico. The content of the Convention was recently modernized, and all original parties have been invited to sign the updated version of the text.⁶³

Brazil

In Brazil, the General Data Protection Law was approved in August 2018.⁶⁴ The law will come into effect after its 18th adaptation period, in early 2020. The law creates a new legal framework for the use of personal data in Brazil, both online and offline, in the private and public sectors. So far, Brazil had a sectoral approach to privacy protections which resulted in conflict of laws.⁶⁵ This new general law aims at providing legal certainty and addressing issues between conflicting laws. The law includes a series of users' rights, provides for specific rules around the processing of sensitive data, and enshrines the principle of purpose limitation.⁶⁶ These measures have the potential to advance meaningful privacy protections for users in Brazil, but these might not be realized due to the lack of an effective and independent enforcement authority. The articles related to the national data protection authority were indeed vetoed by Brazil's president, but a promise was made to create the authority through a separate law.⁶⁷ It is of paramount importance that Brazil follows through and adopts a law establishing an independent authority for the monitoring and enforcement of the data protection law.

Japan

In Japan, a reform of the the country's data protection law was recently concluded. Following this process, Japan was granted an adequacy status by the European Union, to facilitate the flow of data between the two countries.⁶⁸ While the Japanese data protection law may not be perfect and include for instance a limited definition of what constitutes sensitive data, Japan has taken significant steps to increase safeguards for users.⁶⁹

Argentina

In Argentina, a proposal for a new data protection law was introduced in 2018.⁷⁰ Argentina already has a data protection and privacy law and was granted an adequacy status by the EU Commission in 2003.⁷¹ The objective of the new law is to upgrade the level of protection currently in place in the

⁶¹ <http://www.coe.int/web/conventions/full-list/-/conventions/treaty/108>

⁶² https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf

⁶³ <https://www.coe.int/en/web/data-protection/convention108/modernised>

⁶⁴ <https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/>

⁶⁵

[https://uk.practicallaw.thomsonreuters.com/4-520-1732?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhpc=1](https://uk.practicallaw.thomsonreuters.com/4-520-1732?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhpc=1)

⁶⁶ <https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/>

⁶⁷ <https://privacyinternational.org/blog/2233/why-data-protection-authorities-are-essential-cautionary-tale-brazil>

⁶⁸ http://europa.eu/rapid/press-release_IP-18-5433_en.htm

⁶⁹ <https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151289/japan>

⁷⁰ <https://iapp.org/news/a/argentinas-new-bill-on-personal-data-protection/>

⁷¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003D0490&from=DE>

country, and overall the proposal is headed in the right direction despite important shortcomings. Access Now has conducted a thorough analysis of the law and provided a series of recommendations to improve the current proposal.⁷² Importantly, the negotiation process is being conducted behind closed doors, limiting input from civil society and organisations representing users' rights.

United States

In the United States, increasing debates are taking place at state level to increase privacy protection for users. In summer 2018, California passed a privacy bill, signed by the governor in June 2018, which is scheduled to take effect on January 1, 2020.⁷³ Several other states, including Illinois, Vermont, Colorado, New Jersey, Pennsylvania, South Carolina, and New York have passed or are currently pursuing additional privacy protections for their residents.⁷⁴

At the federal level, in the wake of the Cambridge Analytica scandal, members of Congress are either introducing or reviving proposals for new data protection legislation. Some proposals now on the table would only further entrench the prevailing business models that reward unchecked data collection and opaque data exploitation, to the detriment of user rights. Others are a solid starting point for a conversation about what is necessary to provide meaningful data protection and privacy. Below we analyse a number of these proposals in detail.

- **Consumer Privacy Protection Act (S. 2124; H.R. 4081)**

Lawmakers, led by Senator Leahy, introduced the Consumer Privacy Protection Act in 2017. The bill would expand the reach of the the Computer Fraud and Abuse Act (CFAA), which the U.S. Department of Justice has frequently interpreted over-broadly, and also increase the reporting on prosecutions under that law. With regard to privacy protections, it would require the creation of “comprehensive consumer privacy and data security” programs, as well as risk assessments and other internal controls and testing for privacy and security. It would grant more authority to the FTC and allows for investigations by state Attorney Generals. Finally, it includes a section to provide for federal data breach notification for breaches involving sensitive personally identifiable information.

Unfortunately, this approach has several shortcomings. It extends the CFAA without necessary reforms. In some respects, it invokes protections that the FTC has included in consent orders with companies that have engaged in unfair or deceptive trade practices. While this approach isn't bad in theory, it has limited efficacy; Facebook was already subject to many of these provisions under a 2011 consent order. A “self-regulatory” approach fails to provide the rights and obligations that will fully protect users. Further, the law is limited in scope, applying only to entities with data on more than 10,000 U.S. persons, with a carve out for service providers. Finally, while the data breach notification provisions are welcome as one of the most progressive proposals that we've seen, they

⁷²

<https://www.accessnow.org/cms/assets/uploads/2018/09/PROYECTO-DE-LEY-DE-PROTECCIO%CC%81N-DE-DATOS-PERSONALES-EN-ARGENTINA-LO-BUENO-LO-MALO-Y-LO-MEJORABLE-3.pdf>

⁷³

<https://www.forbes.com/sites/stevenbarr/2018/09/17/california-passed-a-new-data-privacy-bill-heres-what-that-means-for-retailers/#5c894dd136e9>

⁷⁴ <https://thehill.com/opinion/technology/402775-states-are-leading-the-way-on-data-privacy>

can be improved, including by giving the FTC authority to develop regulations on the types of data that would trigger notification requirements.

- **BROWSER Act (Balancing the Rights of Web Surfers Equally and Responsibly, H.R. 2520)**

Representative Blackburn introduced the BROWSER Act in 2017. Blackburn is known for, among other things, her opposition to the FCC's separate rules to protect Net Neutrality and the privacy of broadband customers. The BROWSER act requires that internet service providers (ISPs) and "edge" providers (also known in some contexts as "over the top" or "OTT" providers, meaning that they operate over the internet's underlying networks) provide notice of their privacy policies. The bill then provides for opt-in approval for the use, disclosure, or permit access to sensitive information, with opt-out approval for all other information (notably, there is no approval necessary—opt-in or opt-out—for the collection of data). There are several exemptions from these requirements, including a broad one related to "providing" the service or "services necessary to, or used in, the provision of such service."

This is one of the least protective approaches that we have seen in the bills that have been introduced and thus firmly oppose it. Privacy policies have oft proven not to be effective vehicles for protecting privacy. Additionally, the protections given are narrow and largely swallowed by broad exceptions. In addition, the proposal expressly prevents any state from implementing stronger protections, cutting state regulators off at the knees. However, there are some minor positive elements that are worth noting. First, the bill applies evenly to both ISPs and edge providers without exceptions for size or user base, although it doesn't apply to the range of other entities that collect or rely upon massive amounts of sensitive data. Additionally, and most positively, the bill prevents the provision of any service from being conditioned or terminated on the basis of a person's privacy decisions.

- **CONSENT Act (Customer Online Notification for Stopping Edge-provider Network Transgressions, S.2639)**

Senators Markey and Blumenthal recently introduced the CONSENT Act. This bill requires, within a year, for the FTC to promulgate privacy rules for edge providers. The rules must include notification requirements for collection, use, and transmission of certain sensitive data, including personally identifiable information, specification of how data are used and transmitted, and to whom, and protection of de-identified data. The rules also must include opt-in consent for use, transmission, or sale (but not collection) of sensitive information. While it prohibits refusal of service based on unwillingness to provide consent, it does seem to anticipate that other conditions could be imposed by directing the rules to address the reasonableness of prices or discounts related to consent. The bill also requires reasonable data security practices and data breach notification, though only for sensitive information and only if harm is likely.

There is a lot of good in this bill, including a positive notion of opt-in consent. However, it fails to apply to ISPs or any other entity that collects massive amounts of personally identifiable information, making it inherently narrow. Further, outside of the requirement for opt-in consent, it fails to provide adequate guidance in its direction to the FTC, meaning the bill allows for the

promulgation of weak or perfunctory rules. Finally, the data breach notification requirement is a positive step, but by tying it to harm it's potentially too narrow to encompass the full range of risks to user information.

- **MY DATA Act of 2017 (Managing Your Data Against Telecom Abuses Act, S. 964; H.R. 2356)**

Senators Blumenthal and Representative McNerney introduced the MY DATA Act in early 2017. The bill generally states that it is unlawful for a broadband provider or edge provider “to use an unfair or deceptive act or practice relating to privacy or data security,” while directing the FTC to develop implementing regulations and otherwise enforce the Act.

This bill, while positive in its expansion of the FTC’s authority, represents a marginal improvement at best. It doesn’t specify any specific rights or standards to guide the FTC in its promulgation of rules, leaving broad space for ineffective regulations.

- **Secure and Protect Americans’ Data Act (H.R. 3896)**

Representative Schakowsky has led the introduction of the Secure and Protect Americans’ Data Act for the past two congresses. Among other things, the bill provides for the FTC to promulgate regulations on reasonable information security practices, to include regulations on the collection, use, sale, dissemination, and maintenance of personal information, the retention and destruction of personal information, and access to such information. Companies are required to review their policies every year and submit them to the FTC in the case of a data breach, with special requirements for “information brokers”—companies whose business is based around the collection and use of personal data. Additionally the bill has a data breach notification requirement, with notice required within 30 days, and a prohibition on “pre-texting” practices.

While the bill appears at first glance to be a comprehensive approach to data protection, its biggest limitation is that it applies only to “personal information,” which is very narrowly defined. Most notably it excludes some of the most sensitive information that people tend to identify, including photos, personal communications, or the vast scope of information collected by new and developing Internet of Things devices. Further, the bill places too much responsibility for the protection of data on the user themselves, particularly vis-a-vis information brokers, companies which rarely directly interface with users though the bill mostly requires users to visit their websites to exercise their rights.

- **Social Media Privacy Protection and Consumer Rights Act of 2018 (S. 2728)**

The Social Media Privacy Protection and Consumer Rights Act was introduced in April by Senators Klobuchar and Kennedy. The law applies to websites, web applications, and digital applications, including social networks, ad networks, mobile operating systems, search engines, email services, and internet access services. Notably none of these terms are defined in the bill, though “internet access service” is defined elsewhere in U.S. law to exclude telecommunications services (see 47 U.S.C. § 231).

The bill provides for three core protections against these entities. The first relates to transparency and terms of service, and requires notice that personal data produced by the user will be collected and used and an opportunity to prohibit that collection so long as it doesn't render the platform inoperable. Similar notice must be provided in the case of any material change that alters a user's privacy preferences. This disclosure must be made easily accessible and in "clear and concise" language. Further, it requires a privacy and security program that details the use of personal data and explains access to data by employees and contractors. Finally, this first prong requires that a user must be able to withdraw consent to terms of service for use at any time, and when they opt to close their account or terminate use of the platform, their data must be rendered inaccessible in 30 days. The second protection requires that a person has the ability to obtain a copy of their data and a list of persons who received that data from the operator free of charge. Finally, the third protection, relating to privacy violations, requires notice within 72 hours of any violation of a company's privacy or security program or a user's indicated privacy preferences. Such a violation would trigger a direct notice for opt-out from collection or use of personal data (unless it rendered the service inoperable) and allow the user to elect, in regard to personal data tracked by the operator, to have it erased and to cease further dissemination. It would also trigger notice of the user's ability to obtain the copy of their personal data as provided in the second protection. There is an exception to this protection for public safety, and an exception to all three protections in regard to "the development of privacy-enhancing technology." Entities would be required to obtain audits every two years. Enforcement of the full bill is provided for by the FTC, with rights reserved to the States.

This bill has some good ideas, and it is one of the more serious approaches currently before Congress. However, it has a dangerous lack of clarity. For example, while it provides the FTC authority to enforce its terms even as against common carriers, it is unclear to what extent common carriers are included in the bill's scope. Additionally, many of the bill's key protections are also keyed to a triggering event—the creation of an account or use of a website, limiting its protections further, since users may never interact with many of the online entities engaging in intrusive and abusive data practices.

There are several other areas where the bill is detrimentally ambiguous. It provides no definition of data "processing," which is the term that guides the full scope of the second protection. The second protection also seems to apply only to data the user directly provides, and not the invasive profiles created through analysis of that data. In addition there are a host of other undefined terms, like "collection," "use" and "tracked," which delineate the application of other protections, as well as "privacy enhancing technologies" as used in the blanket exception, which could potentially swallow the entirety of the rule. While the bill requires an opt-out for data collection, there is nothing that provides for granularity, seemingly allowing entities to lump the disparate data collection together under a single notice. This would mean that if even one category of data was necessary for the operation of the site, the entity could arguably refuse service if the user decided to exercise the opt-out. And all of this serves as its own example of the shortcoming of requirement for simplicity in an entities' terms of service: such simplicity, without an equivalent requirement to provide more precise detail when requested, could be used to justify even greater ambiguity rather than better user education.

Most importantly, without clarifications, it seems that no part of this bill could have done much to prevent the transfer of data to Cambridge Analytica or provide users with any indication that such a transfer had occurred. These are solvable problems, but they will need to be addressed head-on.

We are encouraged to see these debates in Congress and we believe that privacy and data protection would be better protected with binding obligations for entities processing data, enforceable rights for users and access to remedy. To that end we put forward our proposal for a framework to meaningfully advance privacy and data protection in the U.S. detailed in the above questionnaire (see pages 9 and 10).

- The U.S. has a number of privacy laws that cover conduct by certain entities that collect certain types of information, such as information about consumers' finances or health. Various statutes address personal health data, financial information, children's information, contents of communications, drivers' license data, video viewing data, genetic data, education data, data collected by government agencies, customer proprietary network information, and information collected and used to make certain decisions about consumers. Are there gaps that need to be filled for certain kinds of entities, data, or conduct? Why or why not?
- Does the need for federal privacy legislation depend on the efficacy of emerging legal frameworks at the state level? How much time is needed to assess their effect?

Access Now supports the passage of a comprehensive privacy and data protection law at federal level. Earlier in the submission, we presented our proposal for such a framework. Such a law should not preempt or prevent the creation of any stronger protections that are already written into federal law or exist at the state level.

Broad federal preemption of data privacy laws can stunt innovation and undermine the protection of data. States are more nimble than the federal government and can respond more efficiently and effectively to rapid developments in technology. It is crucial to leave room for states to identify, analyze, and where necessary, respond to emerging gaps in privacy law in the future, which may once again prompt federal action.

Conclusion

We appreciate the FTC engagement with the privacy community. We look forward to continuing to work with your office throughout the series of Hearing and beyond to bring privacy and data protection of users into the 21st century.

Thank you,

Estelle Massé
Global Data Protection Lead
Access Now

Drew Mitnick
Policy Counsel
Access Now

APPENDIX A

Travis Hall, Telecommunications Policy Analyst
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230
Attn: Privacy RFC
(via email at privacyrfc2018@ntia.doc.gov)

November 9, 2018

Re: Developing the Administration's Approach to Consumer Privacy (Docket No. 180821780-8780-01)

Mr. Hall,

Thank you for the opportunity to comment on the National Telecommunications & Information Administration's (NTIA) proposal on data privacy.¹ We welcome the leadership demonstrated by NTIA in this proposal. However, there is still room for improvement. Below we provide general comments on the structure and framing that we believe will better serve NTIA's goals and intent. We then respond to specific questions posed by NTIA.

About Access Now:

Access Now is an international organization that defends and extends the digital rights of users at risk around the world.² By combining innovative policy, user engagement, and direct technical support, we fight for a free and open internet that fosters human rights. As part of this mission we operate a global helpline for users at risk to mitigate specific threats. Additionally, we work directly with lawmakers at national and international forums to ensure policy decisions are focused on users and those most at risk.

General Observations

A. Privacy is about more than consumers

The thrust of the NTIA's proposal specifies the need "to advance consumer privacy." However, in the internet age privacy protections must extend far beyond consumers. Many of the tools and services used by people today are not goods in the traditional sense - people do not pay

¹

<https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy>; *See also* <https://www.federalregister.gov/documents/2018/10/11/2018-22041/developing-the-administrations-approach-to-consumer-privacy> (extending deadline for comment).

² <https://www.accessnow.org/>.

to use them and they do not receive a tangible product. However, this does not mean that there are not significant privacy implications.

For example, users' social media services are probably not "consumers" within the traditional definition, but these services should undoubtedly be subject to any data privacy rules or regulations. Further, while a person may choose to share a piece of information, taken in aggregate millions of data points creates privacy implications at the societal level. Even more troubling online is the passive collection of information from entities like data brokers with whom people may never interact with at all. In fact, these companies may maintain and sell comprehensive data profiles on people who have never heard their name or know they exist. For these reasons, focusing solely on "consumers" is both short sighted and potential harmful to this process. We recommend that the Administration instead focus on the risks to and rights of all people in the United States.

B. Trustworthiness - not trust - should drive data privacy in the United States

NTIA's proposal states, "[u]sers must therefore trust that organizations will respect their interests, understand what is happening with their personal data, and decide whether they are comfortable with this exchange." Counter-intuitively, this framing puts the obligation to act to ensure data privacy on people instead of on the companies themselves. However, rather than people needing to blindly offer trust to companies, it is the companies that must demonstrate that they are worth of receiving and processing user data. It is also the responsibility of companies to provide people with sufficient information in a manner that facilitates their understanding of the scope and purpose of that processing.

As the proposal notes, many Americans have refrained from engaging in important online activities, including economic and civic activities.³ Since this study, the scope and scale of privacy and security incidents have only increased, affecting billions of users of some of the largest companies in the world, from Facebook to Equifax. No amount of trust would have mitigated the harm caused by these incidents, and preventing future breaches requires affirmative efforts from and changes in behaviour from companies.

These are more than pedantic observations. Several of the NTIA's goals are only served if people are served by a data privacy framework, not obligated to it. At the moment, companies are the only entities in a position to take steps to understand the full scope of their data processing, including the third parties who they transmit data to and the various ways they use that data to make decisions about people. A framework that goes beyond checkboxes and compliance mechanisms must respect this reality to drive companies to act in a way that respects and responds to the needs of the people whose data they are using.

³

<https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>

C. A user-centric approach requires that risk is centered on the user

The self-identified “heart” of the NTIA proposal is “risk-based flexibility.” While we emphasize the importance of affirmative rights and obligations, we believe it is important for entities that process data to understand and mitigate risk whenever possible.⁴ However, there are many entities to which risk can be assessed - risk to the data processor, risk to the general public, or risk to the individual person, to name only a few.

Last year, the U.S. National Institute for Standards and Technologies (NIST) published, “an Introduction to Privacy Engineering and Risk Management in Federal Systems.”⁵ A central and vital tenet of that report was the observation that, “[a]n effective privacy risk model must capture the potential cost of problems to individuals.”⁶ In order to ensure that the proposal stays “user centric,” NTIA should follow this model and ensure that the risk management element of the proposal refers specifically and clearly to the risk of the person to whom the data pertains.

Focusing on the person seems like common sense, but the norm has been to focus exclusively on the entity collecting data, not the person whose data was being collected. This meant considering the users only by proxy, in the form of legal or reputational costs. That approach has been wholly inadequate for taking into account the wide range of threats created by data processing, and the harm that may be caused by failure to protect that data (such as the emotional impact of having our personal photos revealed to the world).

D. State-level legislation must be allowed to help drive innovation

Broad federal preemption of data privacy laws will stunt innovation and undermine the protection of data. The NTIA proposal claims “fragmentation naturally disincentivizes innovation by increasing the regulatory costs for products that require scale.” While this may be superficially true, it fails to consider how privacy itself is a driver of innovation, and state laws are drivers of privacy, as we have recently seen with the recently passed California law facilitating national conversations.

States are more nimble than the federal government - either the executive or legislative branches. State legislators can respond more efficiently and effectively to rapid developments in technology. By keeping preemption out of the proposal, or strictly limiting its scope, NTIA will leave room for states to identify, analyze, and where necessary, respond to emerging gaps in privacy law in the future, which may once again prompt federal action.

At the same time it is not assured, as the NTIA proposal implies, that the absence of full federal preemption will lead to meaningful fragmentation. Today, we see several states considering

⁴ See <https://www.accessnow.org/data-protection-in-the-united-states-heres-what-we-need-to-protect-the-users/>.

⁵ <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf>.

⁶ *Id.* See also <https://www.accessnow.org/new-report-helps-u-s-federal-agencies-protect-privacy-companies-use/>.

privacy laws in direct response to the absence of a federal standard. However, a strong national law could remove the pressure of the total absence of protections moving lawmakers to act unless future shifts in technology or business practice require it.

Responses to Request for Comment

A. Privacy Outcomes

NTIA has asked for feedback on the thoroughness and clarity of the privacy outcomes identified in the proposal, as well as any risks that the identified outcomes may pose.

Transparency - To realize transparency as an outcome, the description must expressly extend to transparency into how organizations disclose information to third parties. Any entity that processes data should not only ensure that people easily understand how they process data, but specifically identify any entity that data may be disclosed to, what data may be disclosed, and the nature of the relationship between the entity and the third party. This information shall be proactively communicated to people, who should also be notified of any updates in these practices.

Control - Along with transparency, meaningful user controls to opt into non-necessary data collection and data disclosure practices can empower people. Control should include considerations of social context, including how people interact, or don't interact, with the relevant entity. Further, the proposal would benefit from a more thorough description of what practices may be considered "reasonable," particularly in regard to entities with no first-person relationship to the person about whom data is processed.

Reasonable Minimization - Noting our recommendation that the risk assessed is risk to the person directly, the level of "acceptable risk" determined by the data processor should be disclosed to the person to whom the data relates in a manner that aids understanding of their exposure. Access controls should also be considered as mechanisms to reduce risk.

Security - All data processed by any entity should be secured.

Access and Correction - It is necessary that the proposal include greater detail about what is meant by "qualified access" to personal data. Further, this right should extend not only to the data a person "provides," but to any data pertaining to that person, with exceptions to protect the exercise of human rights. Further, more work should be done to understand what impact deletion rights will have on AI training sets and how to preserve those rights while preserving the ability to use AI tools in a respectful manner.

Risk Management - Any strategy that prioritizes risk mitigation must recognize that there will always be some risk that cannot be mitigated and provide for cessation of any processing that creates risk in excess of what can be controlled.

Accountability - An effective accountability structure must provide a pathway to a private right of action for people who have suffered harm from direct action of a data processor.

Processing and Purpose Limitations - We urge NTIA to include new outcomes for limitations on the bases and purpose for processing data. Data processing should be limited to specific bases, enumerated by law. These may include for example, meaningful, opt-in consent, execution of a contract, or as otherwise necessary under law. The bases for processing data should be identified by the entity, along with the purpose for which that processing is conducted. Acceptable purposes should be prevented from including any use that is discriminatory or has an overly vague description. These purpose limitations must contemplate the most harmful business models - such as those used by data brokers. Without these limitations, the other outcomes fail to provide necessary levels of protection.

B. Proposed High-Level Goals

NTIA has asked for feedback on the thoroughness and clarity of the proposed high-level goals identified in the proposal, as well as any risks that the identified outcomes may pose.

Harmonize the federal landscape; Legal clarity while maintaining the flexibility to innovate - As discussed above, an approach that prohibits state action on privacy governance may stunt privacy innovation and harm users. Further, the identified goal of a “flexible” approach is best realized by providing space for state action in the future. We recommend NTIA prioritize a strong privacy framework over preemption.

Comprehensive application; Scalability - NTIA is correct that protections must apply to all private sector organizations. A truly comprehensive approach should also apply to government and public interest entities. Further, this proposal must extend to all organizations that process data, including third-party vendors, who must be held to the same standards as any other data processor, with few potential exceptions (such as for employee data for small entities).

Employ a risk and outcome-based approach; FTC enforcement - While a risk-based approach may allow for flexibility, such an approach needs to be accompanied by strong penalty provisions as well as agency guidance in the form of interpretive regulations. Without these elements this approach is rife for misuse and abuse. This can be seen in a historic analysis of the European data protection model. Many of the protections in the General Data Protection Regulation (GDPR) are nearly identical to

those in the Data Protection Directive (DPD) that preceded it in 1995. However, companies frequently bypassed or outright ignored the DPD's requirements due to the weak penalties that it carried for non-compliance, as observed in how many changes entities started to implement when GDPR came into force. We strongly encourage NTIA to make strong penalties and regulations an integral part of their proposal.

Interoperability - The most effective method of ensuring international operability is to learn from the approaches of other entities and ensure that the protections contained in a U.S. approach are at least as strong, if not more so. This will not only reduce inefficiencies for data processors needing to comply with multiple legal regimes, but help create certainty for data flows between jurisdictions.

Incentivize Privacy Research - In order to actualize the NTIA's stated goal of "more research into, and development of, products and services that improve privacy protections," we highly recommend pursuit of a program that preferences government procurement of products and services from companies that utilize business methods that are not built or supplemented by personal data or data-driven advertising. Grant programs could also be created that fund entities who are investing in privacy-protective business models and practices or approaches that facilitate interoperability. These programs could be funded through penalties levied on entities who fail to comply with the proposed standards. Government entities can also help by demonstrating a commitment to privacy and security themselves, including committing to protecting and facilitating more robust digital security means and methods and exploring best practices for implementing these provisions in certain sectors, such as the internet of things.

C. Next Steps and Measures

Ultimately, a statutory solution is necessary for ensuring meaningful protection for personal data. However, some measures, like the grant program discussed above, can be adopted by the Administration immediately and have an important impact on the data economy. Further discussions may be helpful in determining the full scope of the proposal, but such discussions need to ensure that representatives across various stakeholder groups are on equal footing to the greatest extent practicable, else corporate interests take over the conversation.

D. Definitions

NTIA's proposal would greatly benefit from inclusion of definitions for various terms, including risk, "reasonable," personal information, and sensitive information, though we recommend that any personal information be treated as sensitive information to prevent an unnecessarily narrow approach to protections. We have provided suggestions for some of these terms throughout this document.

E. Federal Trade Commission Authority

If the Federal Trade Commission is intended to act as the primary regulator for privacy protections, it must be given significantly greater resources and authority to carry out its extended mission.

F./G. International Trade; United States Leadership

Discussions on standards of data protection should be kept separate from trade talks and only included in agreement(s) and arrangement devoted exclusively to transfers of personal data, negotiated by experts in that policy area. By nature, trade policies tend to consider legislations protecting users as a barrier to trade. This creates an inherent push for a lowering of standards to the detriment of rights and the interests of people. A lowering of standards would undermine trust in the digital economy as privacy and data protection laws contribute to the free flow of data globally by ensuring a high level of protection for the information shared and contributing to the security of the infrastructure. Accordingly, we urge NTIA to specify that international trade negotiations or debates at the World Trade Organisation are not a forum to discuss measures for the protection of privacy nor an adequate place were to establish new standards.

Conclusion

We appreciate the NTIA's engagement with the privacy community and trust this feedback will assist the agency in refining and improving its current proposal. We look forward to continuing to work with your office to promote strong data privacy standards.

Thank you,

Amie Stepanovich
U.S. Policy Manager
Access Now

Estelle Massé
Global Data Protection Lead
Access Now

Nathan White
Senior Legislative Manager
Access Now

APPENDIX B



Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
PrivacyFramework@NIST.gov

1 December 2018

Re: Developing a Privacy Framework (Docket No. 181101997-8997-01)

Dear Ms. MacFarland,

Access Now thanks the National Institute of Standards and Technology (“NIST”) for its work to develop a privacy framework to help “identify, assess, manage, and communicate privacy risks.”¹ Earlier this year we warmly welcomed NIST’s report on “An Introduction to Privacy Engineering and Risk Management in Federal Systems,” and we encouraged private entities to adopt its approach.² As such, we are heartened by NIST’s “consensus-driven, open, and collaborative process” and optimistic that NIST can help provide practical paths toward the implementation of meaningful privacy protections.

Protecting privacy is vital in the digital age, where data can be used to manipulate, discriminate against, and harm people. NIST has published a request for information (“RFI”), which grants an opportunity to provide feedback on the goals, framing, and path of the agency’s process. Our comments provide both general observations about NIST’s process to develop the Privacy Framework as well as feedback on specific questions NIST has posed.

About Access Now:

Access Now is an international organization that defends and extends the digital rights of users at risk around the world.³ By combining innovative policy, user engagement, and direct technical support, we fight for a free and open internet that fosters human rights. As part of this mission we operate a global helpline for users at risk to mitigate specific threats. Additionally, we work directly with lawmakers at national and international forums to ensure policy decisions are focused on users and those most at risk.

Access Now has also provided comments to the U.S. National Telecommunications and Information Administration (“NTIA”) on its development of the Administration’s approach to data privacy.⁴ As the RFI indicates, this process is happening in parallel to NIST’s own. We encourage these processes to complement one another and our submissions to both

¹ <https://www.federalregister.gov/documents/2018/11/14/2018-24714/developing-a-privacy-framework>.

² <https://www.accessnow.org/new-report-helps-u-s-federal-agencies-protect-privacy-companies-use/>.

³ <https://www.accessnow.org/>.

⁴ <https://www.accessnow.org/cms/assets/uploads/2018/11/NTIA-Consumer-Privacy-Comments.pdf>.

processes are intended to be mutually-reinforcing. For ease of reference, we also are attaching the full text of that submission here as Appendix A.

In addition, as Appendix B we are attaching “Creating a Data Protection Framework: a Do’s and Don’ts Guide for Lawmakers,” a report written about our experiences working on and supporting the passage and implementation of the General Data Protection Regulation (“GDPR”) of the European Union. Finally, Appendix C contains “A User Guide to Data Protection in the European Union,” a practical guide on rights in the GDPR and how they can be exercised. We hope these resources will provide valuable information about international data privacy standards and practices that will be useful in NIST’s development of a Privacy Framework.

General Observations

A. NIST’s approach must continue to center on the user

In “An Introduction to Privacy Engineering and Risk Management in Federal Systems,” NIST observed, “[a]n effective privacy risk model must capture the potential cost of problems to individuals.”⁵ This was a great victory for user-centric privacy. As we observed at the time:

“Focusing on the user seems like common sense, but the norm has been to focus exclusively on the entity collecting data, not the person whose data was being collected. This meant considering the users only by proxy, in the form of legal or reputational costs. That approach has been wholly inadequate for taking into account the wide range of threats that we face when our data are collected and processed, and the damage breaches can cause (such as the emotional impact of having our personal photos revealed to the world).”⁶

We encourage NIST to commit to carry this principle into the development of the Privacy Framework.

It is important to note, however, that there is no model we are currently aware of to assess individual privacy risks, either on average or specific to a person. Accordingly, more research is necessary in order to determine metrics for evaluating impact before this principle can be properly implemented. NIST should invest in and incentivize this research, which must be expansive and not limited to financial harms. Instead, it must also include emotional, psychological, physiological, human rights, and other impacts that individuals may face on account of a privacy event. It should also include a probe of possibilities for individual and collective remedies, including the options people may have to respond to or mitigate those impacts.

⁵ <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf>.

⁶ <https://www.accessnow.org/new-report-helps-u-s-federal-agencies-protect-privacy-companies-use/>.

Finally, when it comes to the assessment, it should also be noted that risk is often wrongly only considered in relation to the volume of data at risk. Entities processing large amount of data shall indeed have stringent security and privacy obligations, however, this does not necessarily mean small data sets or data processing activities are without risks. Beyond volume, risks must also take into account the type of data, including particularly sensitive data types such as health and biometric, and the amount of information it reveals about a single individual.

B. A risk-based approach to privacy must recognize that some risks are too high to mitigate

As noted in the RFI, NIST held an initial workshop on the Privacy Framework in October 2018 in Austin, Texas.⁷ At that event, speakers appeared to reach consensus that the goal of the NIST process should be to find ways to mitigate privacy risk, but not to get rid of it.⁸ While it may be true, as the speakers agreed, that risk can never be totally eliminated, it is important that the Privacy Framework recognize that some risks are too significant to be properly mitigated and advise that in these cases the activity giving rise to the risk should be forfeited by the entity. NIST should research a method for entities to determine where that threshold exists and identify when a proposed activity reaches it.

Additionally, the principle that the model should assess risks for the individual rather than the entity means that the threshold of acceptable risk should be communicated adequately to the individual, who should be able to exercise a choice about whether to accept that risk, along with steps that can be taken by the individual to mitigate that risk on top of what steps the entity has taken. For choice to be meaningful, alternative solutions shall be provided to individuals who decide that a risk is too high. In today's online environment, individuals encounter many "take it or leave it" approaches whereby they are required to agree to uninformative, complex, or misleading terms and conditions or tracking walls that require consent to tracking in order to use a service. If individuals do not agree to these unilaterally decided conditions, they simply cannot use the service. Such a model fails to both adequately inform the individual and provide meaningful choice. Privacy cannot exist on a "take it or leave it" approach.

A post-hoc example of how this may operate can be evaluated by its absence in the recent data breach at Facebook.⁹ In that instance, to its credit, Facebook quickly notified (albeit inadequately) the population of potentially impacted users after the breach was discovered. However, as we noted at the time:

"[N]either [Facebook's] notice nor the blog post that it links to gives you any information for figuring out whether you specifically have suffered any damage from the breach. Even if Facebook isn't sure yet what, if any, of an individual's information has been compromised, it might have been helpful to advise people

⁷ <https://www.nist.gov/news-events/events/2018/10/kicking-nist-privacy-framework-workshop-1>.

⁸ <https://www.nist.gov/news-events/events/2018/10/kicking-nist-privacy-framework-workshop-1>.

⁹ <https://www.accessnow.org/the-breachbook-chronicles-faq-on-facebooks-latest-privacy-debacle/>.

to review the information they have in their accounts. As the old adage says, it's smart to "hope for the best but prepare for the worst." That should be applied here from the perspective of the impacted users."¹⁰

In the end, no matter what steps a data processing entity may take to mitigate risk, it is the individual who is best placed to understand the extent of a risk and make a decision based on their own context and risk threshold. This is not to say that notification is enough. Notice and choice, as experts have noted at length, is a failed model for protecting privacy.¹¹ Users must have rights to effectively control the processing of their data. There must be an obligation on entities to adequately protect that data, including to meaningfully limit when and to what extent data can be processed.¹² However, where entities are making choices regarding risk thresholds, informing individuals of the factors behind those choices and allowing them to weigh the risk for their own lives empowers people to make more informed, reasonable decisions for themselves.

Specific Responses

A. Minimum Attributes for a Privacy Framework

Consensus-driven and developed and updated through an open, transparent process -

It is too often true that multi-stakeholder processes get captured by the most powerful and well-resourced voices in the room.¹³ NIST must ensure to its fullest capability that all voices are given equal footing in the development of the Privacy Framework. NIST should also recognize that even within a single sector, several groups may disagree about form or substance of a given issue, and take steps to ensure that a multitude of voices are heard and highlighted throughout the process and reflected in the document.

Common and accessible language - We applaud NIST for its commitment to accessible language, which we have found lacking in other government processes.¹⁴ We encourage NIST to follow this through by ensuring that complicated concepts or documents on which the foundation is based are summarized or simplified for a general audience. For example, in places where NIST's Cybersecurity Framework is referenced, it would be good to provide detail on the overlap between the two processes so that an individual does not have to become well versed in one project to participate in this one.

Risk-based, outcome-based, voluntary, and non-prescriptive - We encourage that, among the outcomes presented here, NIST include "effectively protects privacy," or

¹⁰ *Id.*

¹¹ <https://epic.org/2016/07/epic-tells-fcc-to-reject-notic.html>.

¹² <https://www.accessnow.org/data-protection-in-the-united-states-heres-what-we-need-to-protect-the-users/>.

¹³ See, e.g., <https://www EFF.org/document/privacy-advocates-statement-ntia-face-recognition-process>.

¹⁴ See, e.g., <https://www.ntia.doc.gov/files/ntia/access-04202015.pdf> at fn 1 ("For purpose of this comment, we refer to the so called "UAS" as drones throughout, and encourage NTIA to do the same throughout its rulemaking process. In order to adequately involve the public as a stakeholder, it is important to use terms that the public understands and finds accessible. Nondescript acronyms will undermine public involvement and bias respondents toward government, companies, and a small number of civil society groups who understand the issue.").

similar language to indicate action at limiting data processing rather than just encouraging research and innovation.

Compatible with or may be paired with other privacy approaches - The Privacy Framework should aim to take into account the benefits of and learn from the flaws of data protection laws around the world, including the GDPR in the European Union, the Brazilian Internet Law,¹⁵ and other current or soon-to-be passed measures with which entities will have to comply.

B. Goals of the Privacy Framework

The RFI identifies three goals of a Privacy Framework:

- I. To better understand common privacy challenges in the design, operation, and use of products and services that might be addressed through a voluntary Privacy Framework;
- II. to gain a greater awareness about the extent to which organizations are identifying and communicating privacy risk or have incorporated privacy risk management standards, guidelines, and best practices, into their policies and practices; and
- III. to specify high-priority gaps for which privacy guidelines, best practices, and new or revised standards are needed and that could be addressed by the Privacy Framework or a related roadmap.

While we find these to be admirable goals, we also find them to be missing important objectives. As with the outcomes identified above, we don't find that any of the goals identified will actually address privacy challenges that impact users today. Additionally, while now is a crucial moment to establish uniform standards around data protection, neither the identified outcomes nor goals align with, complement, or even recognize those from the NTIA process.¹⁶ For example, the NTIA process includes as goals to incentivize privacy research and FTC enforcement. We encourage NIST to harmonize the identified goals and outcomes with those of the NTIA proposal, along with any subsequent changes in response to public comments.

C. Specific Privacy Practices

One in the list of practices or services NIST expresses interest in receiving information is “de-identification.” Here, we encourage NIST to exercise care in nuance. While information may be de-identified, in that it can be divorced from a specific direct identifier, databases with even a

¹⁵ <https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf>; see also <https://www.accessnow.org/brazil-president-approves-data-protection-bill-but-vetoes-key-accountability-measures>

¹⁶ See, <https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy>; <https://www.federalregister.gov/documents/2018/10/11/2018-22041/developing-the-administrations-approach-to-consumer-privacy> (extending deadline for comment).

small number of data points are often at risk of re-identification with trivial ease.¹⁷ Machine learning tools make this process even easier.¹⁸ However, de-identification is not the only way to protect data: in fact it's only one within a spectrum of methods, including anonymization, wherein steps are taken to prevent re-identification.¹⁹ NIST's inquiry should look beyond simply de-identification to include anonymization and aggregation techniques that will better protect data as artificial intelligence tools continue to advance.

Additionally, NIST also lists "enabling user preferences." Several academics have recently explored the extent that user interface and design decisions impact the ability of people to exercise meaningful choice regarding the use or distribution of their data.²⁰ Recently, a coalition of consumer organisations sent a letter to the Federal Trade Commission calling for an investigation into tech giants deceptive design practices that steer users to "agree" to privacy-invasive default settings.²¹ Any exploration of the existence of user preferences should also include an element of analyzing the design choices that underlie those preferences, including efficacy, intuitiveness, and degrees of nuance, including within the nuance of differing contexts of use.

Conclusion

We appreciate NIST's engagement with the privacy community. We look forward to continuing to work with your office throughout this process.

Thank you,

Amie Stepanovich
U.S. Policy Manager
Access Now

Estelle Massé
Global Data Protection Lead
Access Now

¹⁷ See, e.g.,

<https://www.zdnet.com/article/re-identification-possible-with-australian-de-identified-medicare-and-pbs-open-data>.

¹⁸ See, e.g., <https://journals.openedition.org/factsreports/4494>.

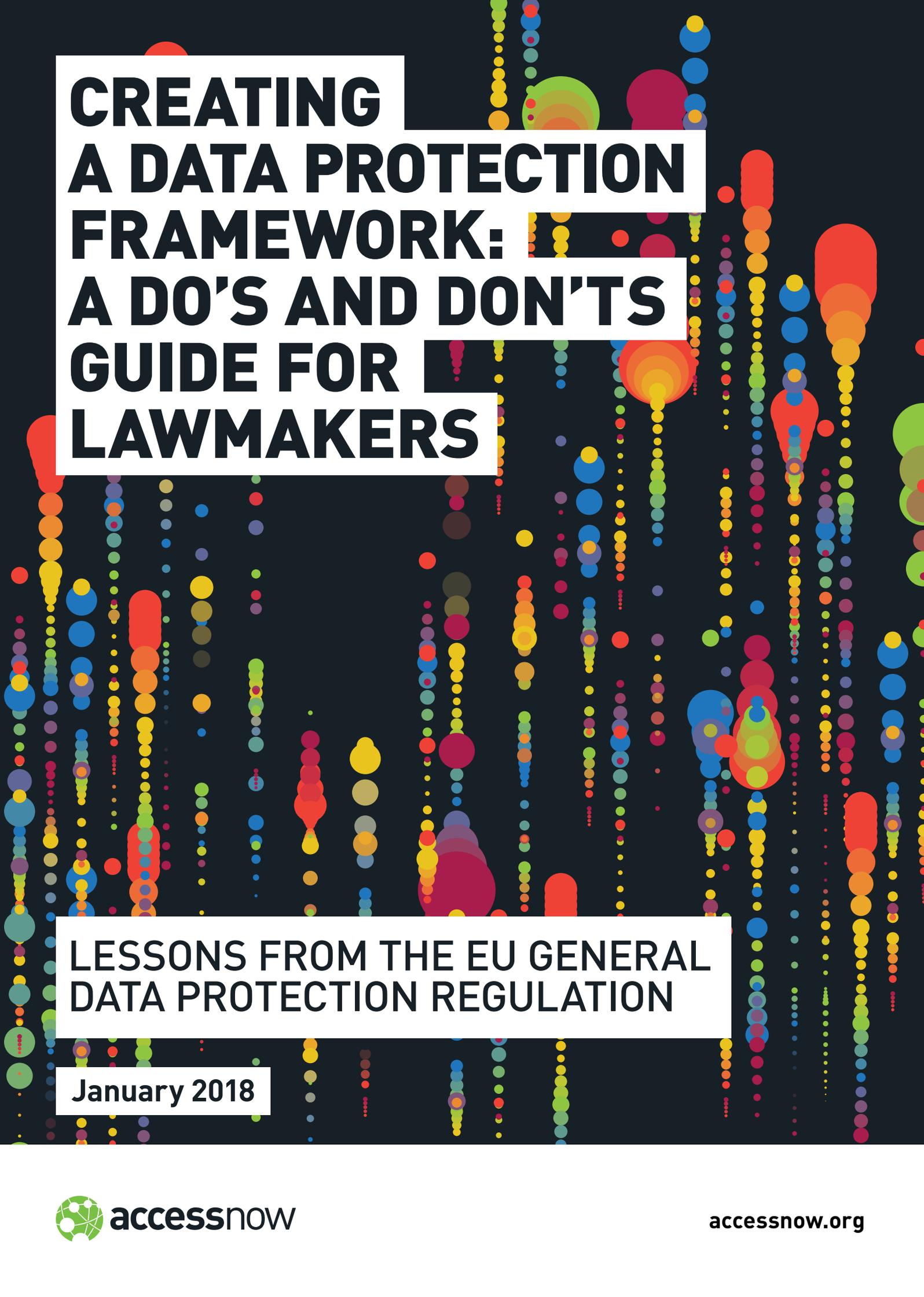
¹⁹ For the spectrum of ways to protect data, see

<https://fpf.org/2016/04/25/a-visual-guide-to-practical-data-de-identification/>.

²⁰ See, e.g., <http://www.hup.harvard.edu/catalog.php?isbn=9780674976009>.

²¹ See, <https://thepublicvoice.org/wp-content/uploads/2018/06/FTC-letter-Deceived-by-Design.pdf>.

APPENDIX C



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

**LESSONS FROM THE EU GENERAL
DATA PROTECTION REGULATION**

January 2018



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.

This paper is an Access Now publication.

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

TABLE OF CONTENTS

● INTRODUCTION.....2

● BACKGROUND.....3

● DO'S.....4

- ① Ensure transparent, inclusive negotiations.....4
- ② Define and include a list of binding data protection principles in the law.....5
- ③ Define legal basis authorising data to be processed.....6
- ④ Include a list of binding users' rights in the law.....6
- ⑤ Define a clear scope of application.....7
- ⑥ Create binding and transparent mechanisms for secure data transfer to third countries.....9
- ⑦ Protect data security and data integrity.....10
- ⑧ Develop data breach prevention and notification mechanisms.....10
- ⑨ Establish independent authority and robust mechanisms for enforcement.....12
- ⑩ Continue protecting data protection and privacy.....13

● DON'TS.....14

- ① Do not seek broad data protection and privacy limitations for national security.....14
- ② Do not authorise processing of personal data based on the legitimate interest of companies without strict limitations.....14
- ③ Do not develop a "right to be forgotten".....15
- ④ Do not authorise companies to gather sensitive data without consent.....17
- ⑤ Do not favor self-regulation and co-regulation mechanisms.....19

● Conclusion.....19

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-trilogues-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.

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.

**Experience
from the GDPR
negotiations**

[17] See UK Information Commissioner's Office, [Data Protection Principles](https://ico.org.uk/for-organisations/guide-to-data-protection/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.

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.

Experience from the GDPR negotiations

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-idUSKCN0ZF1VW>

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.

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 countries²⁷: 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

Experience from the GDPR negotiations

[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.

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.

Experience from the GDPR negotiations

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>

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.

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.

**Experience
from the GDPR
negotiations**

[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)

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?

Experience from the GDPR negotiations

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.

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.

**Experience
from the GDPR
negotiations**

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/TX/?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**

This paper is an Access Now publication.

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

<https://www.accessnow.org>

