U.S. Consumer Privacy Bill Blueprint

[Enforcement and Scope](#)

[Rules for companies](#)
- [Data Minimization](#)
- [Authorized uses](#)
- [Design for Privacy](#)
- [Obligations on Third Parties](#)

[Rights for people](#)
- [Requirements for Consent](#)
- [Right to Rectification](#)
- [Right to Transparency and Access](#)
- [Right to Object](#)

This framework for U.S. privacy legislation outlines clear rules of the road for entities using personal data, details strong rights for people who interact with those entities, and gives the FTC effective authority to make and enforce these rules as technologies evolve. In general, it is designed to shift more of the burden to safeguard personal data from users to companies, and to alleviate the burden on individuals. Ultimately, privacy, security, and data protection are well-served when policy is based upon a comprehensive framework of protections rather than solely technology or sector-specific regulations. Mozilla supports privacy and data protection laws around the world, and the United States has fallen behind on providing similar protections.

Core elements of our proposal:

- A duty of care towards people whose personal data is collected or used by an entity
- Data minimization requirements for data that's no longer necessary for the purpose it was collected
- Purpose limitations that require granular consent for data use and onward transfer
- Clear FTC authority and resources for rulemaking, investigation, and enforcement

Enforcement and Scope

Without effective authority and enforcement, any privacy law will prove ineffective. The FTC currently cannot address all privacy and data security concerns, due to constraints on authority, rulemaking, and resources. Covered entities should be accountable to individuals and enforcement authorities for adhering to these principles.

Covered Data

Any information held by a covered entity that is connected or can be reasonably connected to a person or specific consumer device, with an exception for employee data.[1] Explicit grant of rulemaking to the FTC to determine precise definition of "reasonably connected."[2]

Broad definitions of "personal information" and "sensitive information" that are consistent with the GDPR and allows for the possibility that future advances in technology will expand the definition of what data can be "reasonably connected" to an individual or consumer device.[3]

Covered Entities

Non-sectoral: cover all private entities that handle personal information and are engaged in interstate commerce. Explicit inclusion of common carriers and nonprofits to address gaps in current law. Legislation will not override existing federal sectoral privacy laws such as HIPPA or COPPA.

Rules should be designed to outline rights and prevent specific harms. As more companies across sectors adopt data-driven technology as part of their business, it will be important to establish privacy protections based on how entities collect and use personal data, rather than industry classification.

While this framework does not explicitly address the organization and resources of the FTC, it should be an imperative for Congress to substantially increase the funding and staff of the agency to allow it to

[1] For the purposes of this framework, the terms "information" and "data" are used interchangeably.
[2] Given the recent trend of jurists with a skeptical view of Chevron deference, it will be critically important to explicitly specify grants of agency rulemaking authority.
[3] While this framework does not include a broad delineating principle to distinguish sensitive data, a statutory definition should include information such as unique government identification numbers, financial account or credit/debit card numbers, health information, biometric data, and geolocation data.

provide substantive oversight and enforcement in accordance with its expanded duties.[4]

Preemption

Pre-empt relevant state privacy legislation in order to provide a national standard around data privacy and provide clarity for covered entities.

Pre-emption should be narrowly defined regarding aspects covered by the legislation, and neither the framework nor rules stemming from its authority should pre-empt common law torts, state registries, state data breach laws, or state constitutional guarantees.[5]

In order to justify pre-emption, the baseline bill must include strong user protections and rights, clear rules for private entities, and the additional rulemaking and enforcement tools described in this framework. Otherwise, preemption is not merited.

Rulemaking

Clear rulemaking authority for the FTC to clarify or implement data protection, privacy standards, and responsibilities of data controllers as included in this framework.

This authority provides the agency with the flexibility to address evolving threats to user privacy as technology advances and closes a critical gap in its current enforcement powers.

Duty of loyalty and duty of care

New section for FTC rulemaking authority to ensure that covered entities may not use individual identifying data in ways that could reasonably be expected to harm individuals (regardless of whether the user is also benefitting) and must take reasonable measures to secure their data.[6]

At a minimum, the conception of harm should go beyond mere financial harms to include reputational harm and negative eligibility decisions.

Enforcement

Violations covered under the FTCA, with expanded FTC power to obtain increased civil penalties, both for wrongdoing on a first violation as well as enforcement against repeat offenders. To serve as an effective deterrent, penalties should be levied based on factors such as the

---

[4] *See* Hearing on Oversight of the Federal Trade Commission Before the H. Subcomm. on Digital Commerce & Consumer Protection of the H. Comm. on Energy & Commerce, 115th Cong. (2018) (oral testimony of Commissioner Rebecca Slaughter) (noting that while the economy has doubled in size since the Reagan administration, the FTC has fewer employees today than it did then).

[5] *Cf.* Geier v. American Honda Co., 529 U.S. 861 (2000) (finding that a saving clause alone does not bar the application of conflict pre-emption principles).

[6] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183 (2016).

nature of the violation (particularly the risk to users), the type(s) of data compromised, the magnitude of the compromised data, prior bad acts, and the negligence and/or intent of the entity.[7]

Under the sections associated with this framework, the FTC will have the authority to assess increased monetary penalties that either consistent with the current monetary penalties under Section 5 or may represent a percentage of annual global revenue from offending entities at a maximum. Penalties should be severe enough to serve as an effective deterrent.

Additionally, state AGs should have the ability to pursue violations of the law to protect their constituents. By doing so, the legislation can help reduce any concerns about pre-emption and provide an additional avenue for enforcement if a captured FTC chooses not to act.

Rules for companies

Data Minimization

Personal data should only be collected, stored, used, and shared for purposes that an individual has consented to and for no longer than is necessary for the purposes for which it has been provided.

Purposeful Collection

Covered entities should collect only as much personal data as is reasonably necessary to:

1. provide services or activities that the individual has requested or consented to;
2. enforce the data security or privacy policies of the covered entity; or,
3. other authorized uses as enumerated under this framework.

Definitions of these practices should be determined by the FTC. Authorized uses should be limited to circumstances such as legal compliance or ethical research. Consistent with opt-in for research,

[7] While some have voiced concerns about whether the FTC can be an effective enforcement agency, it is still the most appropriate entity for these responsibilities, given its staff and mission. Among other issues, the FTC has limited civil penalty power under Section 5, which allows the agency to levy penalties only after a final order has been violated--providing bad actors with two bites at the apple. For the FTC to be an effective enforcement agency, it must have the ability to levy penalties independently based on statutory provisions.

	definition must meet standards developed by FTC in consultation with NIST.
Limit Retention	Covered entities should only retain personal data necessary to providing the authorized services or activities, and should delete or de-identify data after that purpose has been fulfilled.
Limit on Use	Covered entities should only use personal data necessary to providing the authorized services or activities. Use of sensitive data should be permitted only to provide the requested user service or for fraud prevention/security purposes.[8] If new requirements exceed the scope of the individual's previous consent or another authorized basis for use, then the covered entity should obtain new consent to engage in that use.
Limit on Data Linking	Personal data collected by multiple distinct entities or parties (data collected by sites or applications not owned by the same party) should not be linked together into one pool of data through unique identifiers without opt-in user consent that clearly specifies data will be linked across multiple, possibly unrelated contexts, subject to exceptions within federal law. This information includes but is not limited to email addresses, advertising identifiers, IP addresses, or random identifiers.
Erasure	Outside of authorized uses, covered entities are obligated to delete personal data based on an individual's request, completion of the purpose collected, or withdrawal of consent. This deletion must be completed within 30 days of request. An individual's request must be subject to verification of identity, proportional to the sensitivity of the data. Additionally, entities must inform users how they handle inactive accounts, including when the account and associated data will be deleted if not used.

Authorized uses

There are a number of expected, or necessary, kinds of processing that entities must be able to engage in - without user consent. A non-exhaustive set of commonly accepted practices, such as those in the FTC's 2012 report, should be explicitly exempted from use restrictions, but not from onward transfer or other secondary use restrictions. These rules should allow sufficient

[8] The FTC will need to prescribe precise limits for the use of data for security and fraud prevention, particularly in light of efforts from some actors to water down current exemptions. *See, e.g.,* Joseph Cox and Jason Koebler, *Data Broker That Sold Phone Locations Used by Bounty Hunters Lobbied FCC to Scrap User Consent*, Motherboard, Jan. 23, 2019, https://motherboard.vice.com/en_us/article/vbwgw8/zumigo-phone-location-data-sold-lobbied-fcc-consent .

flexibility for non-privacy-invasive product features to function, and to enable services to lessen the frequency of consent requests to the end user in the cases of minimal to zero privacy impact. We hope that will encourage more context-appropriate and just-in-time user information around privacy and data practices.

Contract	Necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.[9]
Compliance	Those actions necessary for compliance with a federal, state, or local legal obligation to which the controller is subject.
Financial Logging	Billing and auditing related to the current interaction.
Security	Necessary to protect or defend rights or property against potential security threats, including narrowly scoped fraud prevention.
Imminent danger	To prevent imminent danger to the personal safety of an individual or group of individuals, not to be construed as requiring ongoing surveillance.
Measurement	Analytics and telemetry which does not create a profile based on browsing history, interests, affiliations, or demographics. A profile is defined as a collection of personal aspects of a person that may be used to analyze or predict certain things about them, including but not limited to movement, behavior, health, personal preferences, and interests.
Product fulfillment	Using consumer information to provide order fulfillment would be disclosed by virtue of the transaction itself.
Public interest and research	This law should not overly burden responsible public interest research, as long as opt-outs are respected. In order to fit within this exception, research must also meet ethical standards established by the FTC in consultation with NIST.
Publicly available information	This law is not intended to control publicly available information for non-personalized uses, as long as opt-outs (such as for marketing, including matching public data with personal data) are respected.
Minimal privacy impact	Data use with incidental or no impact on user privacy, such as use outside of a personal context, such as understanding how people

[9] Consistent with established principles of contract law, parties cannot contract around the requirements included within this framework. *See* Restatement (Second) of Contracts § 178 (Am. L. Inst. 1981) (outlining when a contract is unenforceable based on public policy considerations).

interact with a product or service, for instance, to determine why a particular function is not working as intended.

Design for Privacy

Covered entities have an obligation to protect the security and privacy of personal data.

Privacy Impact Assessment	Entities should document the purpose in collecting personal data, the privacy protections and impact for this data, and the potential risk to the individual before collection or a change in the use for collected data. The FTC should create guidance on conducting these design reviews.
Privacy Program	Covered entities should implement necessary organizational processes and practices to fulfill the reasonable expectations and expressed preferences of individuals regarding privacy.
Deceptive or Coercive Design	The FTC will have explicit authority to enforce against deceptive product and service design. In particular, the FTC will have the authority to issue rules and levy penalties regarding the use of dark patterns by covered entities to compel users to divulge personal information, spend money, or share personal contacts (e.g. friend spam).

Obligations on Third Parties

In order to meet the reasonable expectations of individuals, any third parties that a covered entity engages with to use personal data on its behalf, must comply with the rights and preferences of individuals in the same manner as the first party.

Contractual Responsibility	Contracts must include as a minimum the terms requiring the partner to comply with requirements on the first party, including those regarding erasure, data minimization, breach notification, and security. This contract should also prohibit secondary use of the information outside the purposes for which data was shared.

Rights for people

Requirements for Consent

Covered entities should offer individuals with clear and simple choices, presented in a manner that enables individuals to make meaningful decisions about personal data. It is important that consent is granular, in order to address the myriad flaws of a notice-and-consent regime that allows for blanket consent for any data use and onward transfer, and that consent is scaled appropriately to the kinds of personal and sensitive data.

Understandable The process to obtain consent must be clear and distinguishable from other interactions and provided in an easily accessible form, using clear and plain language.

Specific Consent should be obtained in a granular manner and for a particular purpose, so that users provide separate consent for separate uses, not blanket consent for unrelated or ambiguous purposes.

Revocable Individuals have the ability to withdraw consent at any time, and it must be as easy to withdraw consent as it is to give it.

Freely-Given Covered entities should not condition or deny the provision of services based on waiving privacy rights where unnecessary to the fulfillment of the service.

Preserved The terms and conditions provided during the process to obtain consent should be persistently available and archived across versions.

Notified Individuals should be provided with notification of material changes to policies, and consent re-obtained if changes impact the collection or use of personal data.

Recorded Covered entities should be able to demonstrate that the individual provided consent for sensitive or personally-identifiable information.

Right to Rectification

Individuals should be able to correct the data describing them.

Correction Individuals should have mechanisms to correct sensitive information and information used in eligibility decisions to improve the accuracy of such information.

Right to Transparency and Access

Individuals should be provided understandable and comprehensive information describing the collection, storage, sharing, and use of personal data. Individuals should have access to the

personal data that they have provided or generated through a service, and information about the decisions or profiling based on that personal data. This kind of documentation of the design process, and transparency to the user, makes it easier to monitor compliance and understand concerns.

Accountability

Covered entities that collect or use personal data should provide individuals with understandable and comprehensive information, informed by the Privacy Impact Assessment during design, regarding:

1. what personal data they collect from individuals and their purposes for collecting and using that personal data;
2. where personal data regarding an individual is collected from other sources than the individual: the source, categories, purpose, and how to exercise their rights regarding that personal data;
3. when and how they will delete the data or de-identify the personal data from individuals;
4. how their data is used for inferences or decisions based on that data, such as pricing or the provision of services;
5. what conditions or purposes they may share personal data with third parties: the recipients, categories, purpose, and how to exercise their rights regarding that personal data; and,
6. how to exercise their rights regarding that personal data, including how to lodge a complaint with a competent authority.

Data Portability

Individuals should have the ability to export the personal data that they provided or generated via automated processing in a structured, commonly used and machine-readable format at no cost and in a timely manner with the right to transmit that data to another entity without hindrance.

Right to Object

Individuals should be able to exercise control how covered entities use or share the personal data that is collected from and about them, subject to reasonable steps to confirm identity and without an otherwise authorized use.

Opt Out for Marketing

Individuals should have reasonable means to object to the use, profiling, or use of their personal data for marketing purposes.

Opt Out for Research

Individuals should have the ability to object to the profiling or use of their personal data for research studies without de-identification and other experiments. Research under this provision must meet standards for ethical research developed by FTC in consultation with NIST.


moz://a