Responsible Data Practices

EXECUTIVE SUMMARY

A comprehensive US data privacy law, including requirements for responsible data practices, will enable innovative services and unlock benefits for people, organizations, and societies around the world. Google has long championed smart, interoperable, and adaptable data protection regulations—rules that will protect the privacy rights of people and communities and build the trust that enables the digital ecosystem.

There is unprecedented consensus that the US needs a nationwide law to strengthen and guarantee consistent and broadly applicable protections, codify individual rights, and reflect American values. Most agree that America's current privacy regulatory framework, which is composed of sector-specific, consumer protection, and proliferating state laws, is confusing, inconsistent, and expensive. Moreover, many privacy specialists feel that the "notice and choice" approach provides a solid but insufficient foundation for data protection.

So how can we build on that common ground and develop a framework that provides clarity and accountability for companies and organizations and builds trust in the digital ecosystem? We can start with the consensus on what a new federal law should contain, including transparency, data access, deletion, portability, and data security. But many privacy specialists see value in promoting broadly acceptable data collection and handling practices while reducing the need for potentially burdensome consent processes.

This paper considers some common approaches to this question, as proffered in proposals of Members of Congress, civil society, industry, and academia. Some proposals call for total bans on gathering or using certain categories of data or uses; some require default opt-in consent for all or most data collection and use; and still others propose requirements based on the concept of a "duty of care," "data loyalty," or "data fiduciaries."

We believe that it's possible to synthesize these approaches by adhering to responsible data practices, a model that guides our product development. Responsible data practices can be standardized, documented, and embedded into product design and testing to help meet individuals' privacy expectations. Under the responsible data practices standard, organizations that process personal information would take reasonable, affirmative steps to reduce risks to individuals' privacy. This is achieved via a flexible, documented data assessment framework that includes careful consideration of the purposes of data processing, limitations on sensitive or unnecessary data processing, and adoption of privacy-enhancing techniques. This approach harmonizes with well-established principles of legitimate interests, purpose limitation, and accountability in international privacy laws such as the EU's General Data Protection Regulation (GDPR) and the Global Cross-Border Privacy Rules (CBPRs). It also incorporates American legal traditions, including consumer protection standards and the notion of the duty of care.

****

Unlike most of the world's leading economies, the US does not have a national comprehensive data protection or consumer privacy law. Though there are important and effective information and privacy protections built into existing federal sectoral privacy laws, consumer protection laws, state laws, and common law,[1] the US should codify and strengthen consistent protections and individual rights based on universal privacy principles.[2]

We are not alone in this thinking: government entities, industry, civil society, media, and the American people agree that Congress should demonstrate global leadership by passing a law that provides privacy protections for personal information, while enabling responsible innovation, cross-border data flows, and economic growth.[3] Consensus extends beyond the need for a federal law. Experts across political ideologies agree that a federal privacy law should go beyond sole reliance on "notice and choice" as the basis for privacy protection, and towards a more nuanced framework that includes other protections to promote sound privacy practices.[4]

The level and scope of this agreement may be surprising to observers, given that much of the discussion has focused on roadblocks and differences of opinion, specifically relating to the law's scope, coverage, and enforcement. Those are important challenges where thoughtful compromise will be essential. We focus here on how regulation can best strengthen and clarify privacy protections, reduce consent burdens imposed on individuals, and encourage companies to align on and implement best practices. Such regulation should achieve three fundamental objectives:

---

[1] *See, e.g.*, Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506; Health Insurance Portability and Accountability Act, Pub. L. No. 191, 110 Stat. 1936; 201 Mass. Code Regs. 17.01-17.05 (data security standards).

[2] Google called for the passage of comprehensive privacy legislation over a decade ago. *See* Google, Inc., Comment letter to the Department of Commerce on Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (2011) (No. 101214614–0614–01), https://www.ntia.doc.gov/files/ntia/comments/101214614-0614-01/attachments/FINALCommentsonDepartmentofCommercePrivacyGreenPaper%20(3).pdf; Google, Inc., Comment letter to the Department of Commerce on Information Privacy and Innovation in the Internet Economy (June 14, 2010) (No. 100402174-0175-01). And in more recent years, support for such a law has grown. *See, e.g.*, Prepared Statement of the Federal Trade Commission: Oversight of the Federal Trade Commission (May 8, 2019), https://www.ftc.gov/system/files/documents/public_statements/1519212/p180101_house_ec_oversight_testimony_may_8_2019.pdf; Letter from the US Chamber of Congress to Members of the US Congress, Coalition Letter on National Privacy Legislation (Jan. 13, 2022), https://www.uschamber.com/technology/data-privacy/coalition-letter-on-national-privacy-legislation; Eric Null, *We Should Protect Children's Privacy through a Comprehensive Federal Privacy and Civil Rights Bill*, Center for Democracy & Technology (Mar. 22, 2022), https://cdt.org/insights/we-should-protect-childrens-privacy-through-a-comprehensive-federal-privacy-and-civil-rights-bill/; Editorial, *Opinion: Enough failures. We need a federal privacy law.*, Wash. Post, Mar. 30, 2022, https://www.washingtonpost.com/opinions/2022/03/30/congress-must-pass-federal-privacy-law/); Sam Sabin, *States Are Moving on Privacy Bills. Over 4 in 5 voters Want Congress to Prioritize Protection of Online Data*, Morning Consult (Apr. 27, 2021), https://www.washingtonpost.com/opinions/2022/03/30/congress-must-pass-federal-privacy-law/ ("As more states introduce and consider their own data privacy bills, public support for Congress to pass a national standard is holding strong, with 83 percent of voters saying it should be a 'top' or 'important, but lower' congressional priority this year.").

[3] The flow of information now contributes more to GDP growth than the flow of goods. *See* McKinsey Global Institute, Digital Globalization: The New Era of Global Flows, 73 (2016).

[4] *See, e.g.*, Lina M. Kahn, Chair, Fed. Trade Comm'n, Remarks Delivered at IAPP Global Privacy Summit 2022 Wash. D.C. (Apr. 11, 2022) ("I am concerned that present market realities may render the 'notice and consent' paradigm outdated and insufficient."); Christine S. Wilson, Comm'r, Fed. Trade Comm'n, The Role of the Fed. Trade Comm'n in Privacy and Beyond: A Fireside Chat with Comm'rs Rebecca Kelly Slaughter and Christine S. Wilson (Oct. 28, 2019) ("I don't think transparency is the beginning and the end of federal privacy legislation. And I agree with Becca that notice and choice, if at all, has a use only in pretty limited applications."); Rebecca Kelly Slaughter, Comm'r, Fed. Trade Comm'n, FTC Hearing #12: The FTC's Approach to Consumer Privacy (Apr. 10, 2019) (discussing the limitations of the "notice and consent" framework and advocating for solutions that "do not place all or even most of the burden on the consumer"); Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy*, New America (Mar. 23, 2020), https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/ ("Adopting explicit use restrictions for data, as well as defining the rights of users over their own data, will protect privacy better than the current notice and consent framework does. Transparency alone is insufficient."); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1879, 1880 (2013) ("Although privacy self-management is certainly a laudable and necessary component of any regulatory regime, I contend that it is being tasked with doing work beyond its capabilities.").

- First, it should set an appropriate baseline standard of protection that all businesses and organizations that process personal information must meet, guaranteeing substantive privacy rights where there is broad consensus, such as transparency, control, security, data access, deletion, and portability.

- Second, the law should go beyond those substantive baseline standards by holding organizations accountable to embed sound privacy practices into their operations and innovate on the development of new privacy techniques and technologies. The law should make organizations responsible for proactive consideration of privacy issues, rather than relying solely on individual notice and choice.

- Third, while the rules should be clear and predictable, the law should be principles-based to recognize how technology may improve and best practices may evolve. No one wants to have to go back to Congress in a few years needing a new law.

This paper first examines three approaches to privacy and data protection regulation found in US legislative proposals: (1) categorical prohibitions on certain types of data processing; (2) default opt-in consent; and (3) concepts of "duty of care," "data loyalty," or "data fiduciaries." We then consider the approach of responsible data practices, which synthesizes key insights from each of these concepts and other leading international data protection standards. We conclude with a discussion of how one might operationalize the concept of responsible data practices.

Prohibition on Processing of Specific Categories of Personal Information or Activities

To protect individuals by default, some proposals would simply prohibit the processing of specific categories of personal information (e.g., sensitive information such as biometrics) or types of data processing activity (e.g., third-party tracking). The simplicity and clarity of a "red line" approach to data processing can be appealing; individuals and businesses would have certainty on what data processing was and wasn't allowed, and by removing individual choice in certain instances, individuals would be protected from harm without having to consider default settings or put the burden on individuals to make informed choices.

However, outright prohibitions are a very blunt tool and difficult to wield with the precision needed to protect consumers against misuse of data while enabling individually and socially beneficial uses. Prohibitions must be simultaneously broad enough to safeguard against specific harms and narrow enough to avoid significant opportunity costs, such as chilling innovation or cutting off access to beneficial services. For example, DNA profiles are incredibly sensitive and pose significant risk to individuals if they are misused or mishandled, but a ban on processing of genetic information would make impossible services that people value, like the cutting-edge exploration of personalized medicine that has the potential to save millions of lives. Outright bans also limit the kind of consumer autonomy and options strongly protected by American legal traditions. Full prohibitions on types of processing could also undermine explorations of the benefits and harms of the processing. Consider pharmaceutical trials: we don't prohibit the use of a proposed new drug; we allow testing with a small group of people to assess whether a drug is safe and effective, with appropriate guardrails in place to minimize risk.

Outright bans may be appropriate for narrow cases of clearly egregious, undeniably harmful practices, such as use of personal information to unlawfully discriminate against a protected class. But this kind of exception usefully proves the rule: a prohibition on processing specific categories of personal information or activities should be wielded as a scalpel, not as the foundation of a privacy regulatory framework.

Default Opt-In Consent for All or Most Personal Information Collection and Use

Another possible approach is requiring affirmative prior consent for all or most personal information processing. An "all opt-in" approach avoids some downsides of a categorical prohibition, and purports to provide people with control. Most experts agree, however, that an opt-in default standard for all or most data processing does not work in practice. For example, it doesn't account for processing necessary to make products work and ensure they are secure and reliable. Even laws known for their high standard of opt-in consent, like the EU's GDPR, include six bases for processing,[5] like internal operations, fulfilling contracts, or pursuing "legitimate interests."[6]

People generally expect their personal information to be used to provide and improve the services they are using, and for other purposes that are generally considered benign or reasonable in light of their relationship with the organization. Asking people to separately consent to every processing activity heightens the burden on individuals, putting the onus on them to read and understand the implications of hundreds of separate consents, many of which will have only trivial effects. This can have the perverse effect of "'consent fatigue," which some say can lead to "desensitization" in which people click "agree" to everything without paying attention.[7]

Organizations should provide meaningful, easy-to-use mechanisms for individuals to control how personal information is collected and used, including the opportunity to object to processing where feasible in the context of the service. Focusing consent provisions on situations that involve more significant risks because of the sensitivity of the activity (e.g., sale of personal information to a data broker) would allow individuals to focus on making informed choices in those specific instances.

Similar to a prohibition-based approach, an opt-in consent standard should be an aspect of a data protection law, not the foundation for all data processing.

"Duty of Care, "Data Loyalty," or "Data Fiduciaries"

Some have proposed a "duty of care" standard for data protection, placing an enforceable duty on a business to identify and mitigate foreseeable harms that can result from its products or services. This approach has roots in Anglo-American law, which has increasingly expanded protection against harmful conduct even without a contractual relationship between a business and an injured party.[8] The duty of care regime, exercised through the negligence standard in tort law, has been applied to a wide variety of contexts and conduct.

---

[5] GDPR art. 6(1)(a)-(f) (identifying six lawful bases for processing: 1) consent of the data subject, 2) when necessary for the performance of a contract to which the data subject is a party, 3) compliance with a legal obligation, 4) when necessary to protect the vital interests of the data subject or another natural person, 5) when necessary for the performance of a task carried out in the public interest or to exercise official authority vested in the controller, and 6) when necessary for the purposes of the legitimate interests pursued by the controller).

[6] The controller's legitimate interests provide a lawful basis for processing only where the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. *See* GDPR rec. 47. Legitimate interests (which also serve as a lawful basis for data processing under UK law) are likely to be the most appropriate where the controller seeks to use data subjects' data in ways that the data subjects would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. *See* Legitimate Interests, UK Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.

[7] Nicklas Lundblad & Betsy Masiello, *Opt-in Dystopias*, 7 SCRIPTed 155, 163 (2010), https://script-ed.org/wp-content/uploads/2016/07/7-1-Lundblad.pdf.

[8] *See generally MacPherson v. Buick Motor Co.*, 217 N.Y. 382 (1916); *Fowler v. Harper, Fleming James., Jr. & Oscar S. Gray*, Harper, James and Gray on Torts § 12.3 (3d ed. 2021-4 Cum. Supp. 2006-2008); Percy H. Winfield, *The History of Negligence in the Law of Torts*, 42 L. Q. Rev. 184 (1926).

While expanding a duty of care may sound appealing in terms of shifting responsibility for protecting privacy from individuals to organizations, it has not proven to be a useful model for a general privacy law (apart from the requirement of reasonable data security safeguards—which is similar to a negligence standard). The principal objection to using negligence law as a basis for privacy is the difficulty in identifying harms in the privacy space.[9] Negligence claims are generally focused on concrete, tangible harms like physical injury or financial loss. Privacy claims can allege violations of individual rights that are often hard to define in terms of tangible harm, like incursions into autonomy or loss of control. As Danielle Citron and Daniel Solove observed, privacy harms "often involve future uses of personal data that vary widely" and are difficult to predict or quantify.[10]

The "duty of loyalty" or "fiduciary duty" concept is a related approach that comes out of the special relationships individuals have with trusted providers like lawyers, trustees, or certain financial managers, where individuals place trust in an expert to manage some aspect of their affairs.[11] Some scholars, most notably Woody Hartzog and Neil Richards, have proposed using "data loyalty" to shift responsibility in privacy law, altering the relationships between individuals and organizations, and requiring organizations to act solely in the interests of individuals.[12]

The concept has proven better suited for the one-to-one context, in which an expert provider has a specific relationship with an individual and can assess their best interests, than for modern commercial interactions. In today's economy, consumers interact at arm's length with organizations that must balance individual interests and collective benefits to other users, as well the interests of an ecosystem of merchants, content creators, rivals, and more.[13]

Responsible Data Practices

The above approaches aim at expanding organizations' responsibility for establishing a base level of privacy protection. But all have issues that limit their utility as a general solution for US privacy law that can be easily understood, broadly applied, and support continued innovation. The principle of responsible data practices draws on these concepts, while minimizing their limitations. Responsible data practices also echoes the risk-based model that provides the foundation for global privacy frameworks like the GDPR and the Global CBPRs.[14]

---

[9] *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. Rev. 793, 816 (2022). In addition, while negligence makes sense as a standard applicable to unintentional conduct that causes harm (such as lax security practices that cause unauthorized access and misuse of sensitive personal information), it is a poor fit for intended actions, such as the sale of data to a data broker.

[10] *See id.* at 793.

[11] *See, e.g.*, Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. Corp. L. 143, 144-45 (2020) (arguing that "consumer transactions in the information age should create fiduciary relationships between consumer and company" such that "companies would have fiduciary duties to consumers that consumers cannot waive, regardless of boilerplate's text"); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183, 1209 (2016) ("An information fiduciary is a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship.").

[12] *See* Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 Wash. U. L. Rev. 961, 967 (2020) (arguing for the duty of loyalty as a better approach than a notice and choice model); Jack M. Balkin & Jonathan Zittrain, A Grand Bargain to Make Tech Companies Trustworthy, The Atlantic (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ (arguing for fiduciary obligations for online service providers); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183, 1186 (2016) (arguing that many online service providers and cloud companies that collect, analyze, use, sell, and distribute personal information are information fiduciaries).

[13] *See, e.g.*, Alessandro Acquisti et al., *The Economics of Privacy*, 54 J. Econ. Literature 442, 462 (2016) (explaining that "the economic consequences of less privacy and more information sharing for the parties involved (the data subject and the actual or potential data holder) can in some cases be welfare enhancing, while, in others, welfare diminishing," and noting that "in choosing the balance between sharing or hiding personal information (and in choosing the balance between exploiting or protecting individuals' data), both individuals and organizations face complex, often ambiguous, and sometimes intangible trade-offs").

[14] *See* Cross-Border Privacy Rules System, http://cbprs.org/.

As described above, the GDPR requires opt-in consent for specific processing activities, but provides a number of legal bases on which organizations can rely when processing personal information. Specifically, the GDPR permits data processing for purposes that are not incompatible with the individual's rights and interests,[15] and where "processing is necessary for the purposes of the legitimate interests pursued by the controller."[16] This "legitimate interests" test allows organizations to process personal information for purposes like research and development and product improvement. The legitimate interest basis for data processing appropriately bounds the processing of personal information in ways people expect in the context of a service, without requiring a specific consent for more typical, expected uses like product improvement or basic analytics. In contrast, the GDPR requires opt-in consent only in limited, higher-risk circumstances, helping to combat "consent fatigue."

The CBPR system requires organizations to be accountable for compliance with the program requirements by documenting their privacy practices and being able to demonstrate to an expert, independent authority that their data processing does not pose undue risk to individuals. This accountability principle is the linchpin of ensuring that organizations do their work, but doesn't prescribe the specific manner in which the work must be done.

The notion of responsible data practices should also be familiar under American legal standards, as it requires organizations to engage in a process of understanding and attempting to mitigate the risks posed by the processing of personal information. It thus has similarities to the legal tradition of the duty of care, and the proposals from Senator Schatz[17] and Senator Cantwell.[18]

Requiring reasonable data practices would mean requiring organizations to **take reasonable steps to identify the relevant interests and risks involved in the processing of personal information, implement a program or plan designed to minimize those risks consistent with the context of the applicable services, and document this process as part of an overall privacy assessment to enable accountability**. This responsible data practices concept can promote a private-by-design approach that furthers the substantive requirements of a comprehensive privacy law, including obligations of transparency, control, access, deletion, portability, and data security.

Operationalizing Responsible Data Practices

All organizations should take reasonable steps to understand the relevant interests and risks involved in their data processing operations. This includes individual and collective interests, including free expression, interoperability of services, service efficiency and reliability, etc. This process can be quite simple for organizations that have limited or standardized processing of personal information, or more complex for those that operate a range of services for large numbers of users. Organizations should then take reasonable steps to review the purposes and means of processing and identify what steps it can take to address and reduce related privacy risks.

This process should be familiar to those operating under international regimes like the GDPR, and should be made simple for smaller companies. This process is often referred to as a data protection assessment

---

[15] GDPR art. 5(b).
[16] GDPR art. 6(1)(f). *See also*, Centre for Information Policy Leadership, How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation, July 2021, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf.
[17] Senator Brian Schatz, Data Care Act of 2021, S. 919, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/919.
[18] Senator Maria Cantwell, Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/2968.

and is a bedrock of accountability under many existing data protection laws. A privacy assessment allows a regulator to hold an organization accountable if violations or problems occur, without having to approve processing in advance or impose other procedural hurdles that limit flexibility and innovation. A key notion here is that the assessment should be a *reasonable* attempt to address risks. It does not require that an organization got it perfectly right in hindsight, but rather that, in the aggregate, it had reasonable systems and processes in place.

Reasonable privacy practices recognize that there are an infinite variety of processing activities and organizations—from big tech companies to small retail outlets. Each organization should assess its own context for its data processing. Organizations and industries can standardize this process for typical data uses, and regulators and experts can help to define both interests and potential harms through guidance.

One way of minimizing risk is via "data minimization," limiting the purposes and means of collection, use, and disclosure of individuals' personal information to what is reasonably necessary and proportionate to provide the service or product, or is otherwise consistent with the context of an individual's relationship with the data controller.[19]

What might this look like in practice? First, where feasible, organizations should strive to use less identifying information, including taking approaches like use of pseudonymous or de-identified information. Second, organizations should avoid or limit processing of inherently sensitive or higher risk personal information (e.g., health information or biometrics) where less sensitive information can be used while providing the same level of functionality and security.

Organizations should, where possible, also leverage privacy-preserving technologies (PPTs)[20] that can enable them to offer services, features, and goods with higher levels of privacy. Going beyond "private by design" to "private by innovation," techniques like federated learning and federated analytics allow organizations to leverage the benefits of learning from real-world interactions with individuals without actually collecting user data, enabling more accurate and robust applications while minimizing data collection and potential risks.

We applaud Senators Cortez-Masto's and Fischer's leadership on this issue with their bipartisan legislation,[21] and the US-UK International Grand Challenges on Democracy-Affirming Technologies[22] that would support state-of-the-art PPTs and promote their responsible use. Further investments from Congress and others will enable research into techniques and protocols to enable effective and beneficial uses of personal information while protecting personal information.

****

[19] A data controller determines the purposes and means of processing data—what data to collect and how to process it. GDPR, art. 4. *See also* Controllers and Processors, Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/ (data controllers are "the main decision-makers" and the ones that "exercise overall control over the purposes and means of the processing of personal data").

[20] PPTs, sometimes called privacy-enhancing technologies (PETs), are technologies that use approaches likee data minimization, anonymization, and pseudonymization to increase privacy protections without compromising the functionality of the processing activity, such as encryption and pseudonymization. *See Privacy Enhancing Technologies*, ENISA, https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies.

[21] *See* Promoting Digital Privacy Technologies Act, S. 224, 117th Cong. (2021), https://www.congress.gov/117/bills/s224/BILLS-117s224is.pdf.

[22] *See* Press Release, The White House, US and UK to Partner on Prize Challenges to Advance Privacy-Enhancing Technologies (Dec. 8, 2021), https://www.whitehouse.gov/ostp/news-updates/2021/12/08/us-and-uk-to-partner-on-a-prize-challenges-to-advance-privacy-enhancing-technologies/.

A US comprehensive federal privacy law should begin with consensus principles like transparency, data access, deletion, portability, and data security. A federal privacy law must also move beyond "notice and choice" as the sole basis for privacy protection toward a framework based on responsible data practices. Such a framework will set an appropriate baseline of data protection, better share the responsibility for protecting privacy between individuals and organizations, and be principles-based, allowing it to adapt to changes in technology and evolving best practices.

Satisfactory solutions to privacy challenges will require ongoing commitment, and our work in this space will not end once a federal law is in place. We will do our part to improve the ecosystem—ensuring individuals are protected and businesses and organizations have an opportunity to innovate and grow—and responsible data practices will be at the core of this work.

****