Safe Harbor Provisions

According to Cornell Law School, a safe harbor is "A provision granting protection from liability or penalty if certain conditions are met. A safe harbor provision may be included in statutes or regulations to give peace of mind to good-faith actors who might otherwise violate the law on technicalities beyond their reasonable control." Thus safe harbors have a valuable role in making privacy legislation less adversarial towards covered entities and raising awareness of best privacy practices. In relevant laws there are four primary forms these safe harbor provisions take that can help inform a federal privacy law. These refer to the right to cure, reasonable security, international transfer, and third party transfer provisions, all of which have certain advantages and disadvantages for protecting privacy while also not unduly harming covered entities.

The right to cure requires a data subject to notify a covered entity of the violation it intends to sue for and gives said entity a certain time period to "cure" this violation before they can pursue some form of legal action. In the case of the California Consumer Protection Act (CCPA) this protects against statutory damages but this could also be written to protect a covered entity from all civil liability.

A reasonable security safe harbor provides covered entities with some form of protection against liability or reduces fines if they meet a certain standard. This standard may be vague and leave the interpretation of reasonable security up to the courts as in the case of the CCPA, or it may be specific and provide exact frameworks or certifications to be used to provide a safe harbor from liability as in the case of the Ohio Data Protection Act. In the case of specific standards, these may be determined by Congress, the Federal Trade Commission (FTC), or FTC approved gatekeepers.

A safe harbor for international transfers protects against liability for covered entities that transfer data to other countries if a certain level of privacy protection is also present in that country. This level of protection is generally left up to the interpretation of the courts and can change as was seen with the Schrems I and II cases in regards to EU transfers to the US.

A safe harbor for third party transfers protects against liability for covered entities that transfer data to a third party who then commits a violation if they ensure certain security standards. These can vary but generally it requires a written contract detailing the obligations the third party has to protect the data and that the covered entity did not have knowledge of the violation occurring as seen in the CCPA.

Also listed below is a selection of relevant examples of these different provisions. These are certainly not exhaustive, but they provide a framework for examining the specific legal language that may exist in a federal privacy law.

Right to Cure

Advantages

- Allows covered entities a time period in which to correct their mistakes and avoid fines or litigation for a harm they did not intend to commit. (CCPA)

- In the case of a federal privacy law this would provide a counterbalance to the private right of action as the "Right to Cure" would protect a covered entity from certain damages if they fix their violation. This provides an incentive to reform bad data privacy actions to prevent litigation. (CCPA, Rosenthal)

    - This does not protect against a lawsuit for actual damages in CCPA, it merely protects against statutory damages. However, actual damages are a much more amorphous concept in terms of privacy violations which leaves a large amount of interpretation powers to courts.

Disadvantages

- This can allow covered entities to escape liability for their actions by curing their mistake even if damage was still done to the data subject or if the entity was knowingly negligent. This relates to the broader debate on remedies, whether the law should aim to deter actions by imposing costs or by providing safe harbor options that forgive mistakes. (CRPA)

    - The court interpretation of what is a cure here is crucial. As seen below, California courts interpret a right to cure as requiring the negative effects of the violation to be remedied. What constitutes a remedy in the context of data violations may be a thorny legal issue that leaves a lot of ambiguity in determining whether a cure has been achieved and thus whether a private right of action is possible. (Romero)

    - CRPA notably gives the California Privacy Protection Agency the ability to give a covered entity a right to cure at their discretion largely dependent on intent.

Reasonable Security

Vague Conditions (More Consumer Friendly)

Advantages

- Interpretation is done on a case by case basis, providing more flexibility in how good faith is interpreted and helping ensure a company actually has good practices. (CCPA, 35 U.S.C. § 271, ACPA)

· Will encourage covered entities to provide a best effort in terms of consumer privacy to avoid potentially opening themselves up to litigation or to reduce the size of fines.

Disadvantages:

· Lack of standards makes it hard for covered entities to meet the required level of security. (CCPA)

· Covered entities may not use the safe harbor because of this vagueness, rendering it relatively ineffective. (ACPA)

· Generally, it is more expensive for covered entities to meet these standards.

Specific Conditions (More Business Friendly)

Advantages

· Gives covered entities a clear standard to meet, thus encouraging documentation of privacy steps and making it easier for them to take responsible data security measures to avoid litigation. (TCPA, Ohio, Connecticut, Utah)

· Generally, it is cheaper and easier for covered entities to meet these standards.

· A certification process allows for more industry input balancing the rights of consumers and covered entities in determining a safe harbor. (COPPA)

Disadvantages

· May contain standards that are too low thus creating a ceiling for privacy. This can allow covered entities to escape liability for a breach of consumer data by simply meeting a baseline standard and taking no other security steps.

  o This is particularly relevant in the case of frameworks as opposed to a certification process. Certifications tend to require an organization to judge that the standards a covered entity has implemented are appropriate within a certain scope while a framework like NIST standards is an exact definition of exactly what is required. (Ohio DPA vs COPPA)

·

International Transfers

Advantages

- Provides a clear framework for international data transfers reducing costs and ensuring smooth business functioning for covered entities that operate internationally. (Uzbekistan, GDPR)

- Helps reduce friction with neighboring countries over data privacy by synchronizing similar laws.

Disadvantages

- Meeting an “adequate” or “essentially equivalent” level of protection may be difficult and can be reinterpreted by courts. (Schrems I, Schrems II)

- May pose security risks from international transfers if the country receiving the data does not have as strong of privacy regulations as believed or if the government of said country violates those protections.

Third Party Transfers

Advantages

- Provides a clear framework for third party transfers ensuring companies have a way of avoiding liability for third party violations they had no reasonable way of preventing (CCPA, GDPR).

- If a stricter liability is used, it encourages covered entities to constantly monitor the actions of a third party to whom they transfer data. (GDPR)

Disadvantages

- Depending on the level of liability for third party violations this may encourage less regulation and oversight of third parties to whom data is transferred so the covered entity avoids opening themselves up to litigation. (CCPA)

- If a stricter liability is used, this may significantly increase the costs of regulation to constantly monitor compliance of third parties. (GDPR)

Examples

Right to Cure

CCPA: Gives businesses time to correct violations before private right of action is possible. However, this provision was removed in the CRPA and thus will no longer be valid beginning in 2023

"If you want to sue for statutory damages, you must give the business written notice of which CCPA sections it violated and give it 30 days to give you a written statement that it has cured the violations in your notice and that no further violations will occur. You cannot sue for statutory damages for a CCPA violation if the business is able to cure the violation and gives you its written statement that it has done so, unless the business continues to violate the CCPA contrary to its statement."

https://oag.ca.gov/privacy/ccpa

Rosenthal Fair Debt Collection Practices Act: Rosenthal does not require a business to receive notice of the violation but also gives them the ability to cure a violation if they discover it themselves.

"A debt collector shall have no civil liability under this title if, within 15 days either after discovering a violation which is able to be cured, or after the receipt of a written notice of such violation, the debt collector notifies the debtor of the violation, and makes whatever adjustments or corrections are necessary to cure the violation with respect to the debtor."

https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.6C.&part=4.&chapter=&article=1.

Romero v. Dep't Stores Nat'l Bank: Provides a specific legal definition of a "cure" in California requiring ill effects to be remedied. In the case of a data breach this means even if a covered entity fixes the vulnerability that allowed a breach, if other negative effects occurred that they are unable to fix they are still liable

"That California would require a creditor to return a debtor to the position she was in before the Rosenthal Act violation in order to "cure" that violation finds support in other contexts, where future compliance is an insufficient "cure" if the ill effects of a violation have not been or cannot be remedied."

https://cdn.ca9.uscourts.gov/datastore/memoranda/2018/02/28/16-56265.pdf

Reasonable Security

35 U.S.C. § 271(e)(1): Safe Harbor Provisions in drug manufacturing, much of the interpretation is left up to courts.

"[E]vidence of intent can be a relevant factor in determining whether an activity is reasonably related to obtaining FDA approval, and that [*Abtox* and similar cases] stand for the proposition that evidence of commercial intent is not determinative of the safe harbor inquiry." *Amgen Inc., et al. v. Hospira, Inc*., Case No. 15-cv-839-RGA (Order, August 27, 2018)

https://www.jdsupra.com/legalnews/safe-harbor-provision-of-35-u-s-c-271-e-75236/

35 U.S.C. § 271(e)(1) ("It shall not be an act of infringement to make, use, offer for sell, or sell within the United States a patented invention . . . solely for uses reasonably related to the development and submission of information under a Federal law which regulates the manufacture, use, or sale of drugs or veterinary biological products."

https://www.law.cornell.edu/uscode/text/35/271

CCPA: Reasonable security not defined, left up to courts to interpret if this standard is met or can be faced with statutory damages.

"[a]ny consumer whose nonencrypted and nonredacted personal information . . . is subject to unauthorized access and exfiltration, theft or disclosure as a result of the business's violation of the duty to implement and maintain **reasonable security** procedures and practices appropriate to the nature of the information to protect the personal information"

https://oag.ca.gov/privacy/ccpa

ACPA: Similar vagueness of safe harbor means it's not often used

"Accordingly, the court's inquiry usually centers around determining whether a defendant showed a bad-faith intent to profit . . . the court has wide latitude to discern bad-faith intent from the facts of each case. Furthermore, the ACPA provides a legislative safe harbor for those defendants who "believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful. Thus, either an absence of bad-faith intent to profit, or a genuine and reasonable belief that one's use of a domain name is legitimate, will preclude liability under the ACPA.

However, in practice, defendants rarely invoke the legislative safe harbor, perhaps because of the more nebulous nature of the fair use defense."

https://lawcat.berkeley.edu/record/1119829/files/fulltext.pdf

TCPA: Defines specific conditions a company must meet to qualify for safe harbors

"a safe harbor from liability for the good faith blocking of illegal and unwanted robocalls . . . The first safe harbor protects phone companies that use reasonable analytics, based in part on caller ID authentication information, to identify and block illegal or unwanted calls from liability. Currently, only STIR/SHAKEN authentication satisfies this requirement. . . . The second safe harbor protects providers that block call traffic from bad actor upstream voice service providers that pass illegal or unwanted calls along to other providers, when those upstream providers have been notified but fail to take action to stop these calls. Because this safe harbor will focus on known bad actors — upstream voice service providers that are

facilitating, or at a minimum shielding, parties originating illegal calls — it will not rely on consumer consent."

https://www.natlawreview.com/article/tcpa-regulatory-update-fcc-adopts-safe-harbor-to-encourage-blocking-unwanted

"damages can be reduced in cases where the caller has implemented a documented system for reasonable compliance"

https://poseidon01.ssrn.com/delivery.php?ID=158006120027098087066123122115096023022073004041071075072106111101110064002122078099004009106006041043008021112095090002127120027034008006040082029027024007114072073016004070109090001102116080006093003003092078116112016087117093094110087020078021074&EXT=pdf&INDEX=TRUE

COPPA: Organization must receive certification from an FTC approved program to be eligible for the safe harbor. This certification must be kept up to date or the safe harbor is not valid as seen in the FTC's actions against Miniclip.

"The COPPA Rule includes a safe harbor provision that allows industry groups and others to seek FTC approval for self-regulatory guidelines that implement protections that are "the same or greater" than the COPPA Rule. A company is deemed to be in compliance with COPPA if it's a member of an FTC-approved COPPA safe harbor program and honor its guidelines."

https://www.ftc.gov/news-events/blogs/business-blog/2020/05/do-your-coppa-safe-harbor-claims-hold-water

Ohio DPA: Similar to TCPA, this provides a specific set of actions a company can take to qualify for safe harbor and have an **Affirmative Defense**. However, these standards may be too low as they only require meeting a security framework such as NIST or HIPAA and nothing else.

"(A) A covered entity seeking an affirmative defense under sections 1354.01 to 1354.05 of the Revised Code shall do one of the following: (1) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that reasonably conforms to an industry recognized cybersecurity framework, as described in section 1354.03 of the Revised Code; or (2) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of both personal information and restricted information and that reasonably conforms to an industry recognized cybersecurity framework"

https://codes.ohio.gov/ohio-revised-code/section-1354.02

HIPAA: When determining size of fine for HIPAA violations the security measures the covered entity took should be considered as a mitigating factor

"When making determinations relating to fines under such section 1176 (as amended by section 13410) or such section 1177, decreasing the length and extent of an audit under section 13411, or remedies otherwise agreed to by the Secretary, the Secretary shall consider whether the covered entity or business associate has adequately demonstrated that it had, for not less than the previous 12 months, recognized security practices in place that may (1) mitigate fines under section 1176 of the Social Security Act (as amended by section 13410); (2) result in the early, favorable termination of an audit under section 13411; and (3) mitigate the remedies that would otherwise be agreed to in any agreement with respect to resolving potential violations of the HIPAA Security rule"

https://www.congress.gov/bill/116th-congress/house-bill/7898/text

Utah H.B.80: Similar to Ohio DPA requires meeting of security frameworks such as NIST or FedRAMP. Also must be of "appropriate scale and scope" to have an affirmative defense.

"A person that creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of Subsection (4), and is in place at the time of a breach of system security of the person, has an affirmative defense."

https://le.utah.gov/~2021/bills/static/HB0080.html

Connecticut H.B.6607: Essentially same as Ohio and Utah, must have "reasonable cybersecurity controls for safe harbor

"To incentivize the adoption of cybersecurity standards for businesses by allowing businesses that adopt certain cybersecurity framework to plead an affirmative defense to any cause of action that alleges that a failure to implement reasonable cybersecurity controls resulted in a data breach concerning personal or restricted information."

https://cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&which_year=2021&bill_num=6607

International Transfers

GDPR: Requires adequate level of protection the standard of which is left up to interpretation for the Commission

"A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an **adequate level of protection."**

CCPA: Proposal that there should be safe harbor between CCPA and GDPR (or a US federal privacy legislation. This was not adopted and thus California still has the same legality issues stemming from EU-US transfers.

"The GDPR offers many protections for California consumers that the CCPA does not. Thus, it's likely that if consumers actually understood both laws, many California consumers would

regard the GDPR as equal or superior to the CCPA at protecting their interests. Meanwhile, everyone—including consumers—would benefit from the "significant economies of scale" and associated cost reductions that would come from a GDPR-compliance safe harbor to the CCPA."

https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3093&context=historical

Schrems I: Requires "essentially equivalent" level of data protection for any country to meet the safe harbor provision of the EU

"The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter."

https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=143358

Uzbekistan Data Protection Law: Similar standard but wording is adequate protection vs essentially equivalent

"Cross-border transfer of personal data is carried out to the territory of foreign states that provide adequate protection of the rights of subjects of personal data." (translated)

https://lex.uz/docs/4396428

Third Party Transfers

CCPA: A covered entity is not liable if a third party whom they transfer data to under a contract that meets certain standards violates said contract

"A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation."

https://oag.ca.gov/privacy/ccpa

GDPR: Stricter interpretation, the data controller may still be liable for violations by a data processor they use even if there is a contract in place as they should constantly be monitoring the processors compliance through audits.

“Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.”

“makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.”

Safe Harbor Definition: https://www.law.cornell.edu/wex/safe_harbor