1. Breach of contract and warranties litigation

By Cheryl Saniuk-Heinig, CIPP/E, CIPP/US

The data privacy litigation landscape in the U.S. has seen a rise in lawsuits brought by private individuals for privacy violations under theories of breach of contract and breach of warranty. These legal claims are often the result of privacy incidents or violations and seek to leverage a company's own privacy notice, terms of service, advertisements or other public statements as contractual commitments or assurances.

Breach of contract and breach of warranty claims have a long-standing history as causes of action and have generated an enormous amount of relevant case law before plaintiffs began raising arguments in the context of privacy incidents. This analysis will cover four types of claims — breach of express contract, breach of implied contract, breach of express warranty and breach of implied warranty — and discuss the strategies plaintiffs have used, both successfully and unsuccessfully, to advance these claims in court.

Breach of express contract

An express contract forms when competent parties reach a meeting of minds and explicitly state their terms either orally or in writing and said terms create mutual obligations upon the parties. The concept of an express contract dates back centuries, and courts typically find them enforceable based on clear, agreed-upon promises.

Today, express contracts can include service agreements, employment contracts and commercial transactions. These contracts require clear duties such as access, payment terms and timelines.

Breach of implied contract

A contract does not always need to be written to be enforceable. Courts have long recognized that contractual obligations can arise from behavior or circumstances signaling a mutual intention between parties to form a contract, even if no written or spoken terms are agreed upon.

Depending on the circumstances, implied contracts can be invoked in service transactions where the nature of the parties' interactions and conduct implies an agreement. For example, some impacted patients have claimed breach of an implied contract when a health care provider advertised a commitment to keeping all

patient data secure through "industry-leading practices" but inadequate security measures exposed patient data. They argued the provider implicitly promised to safeguard their data and, by collecting sensitive information, had an implied duty to protect it.

Breach of express warranty

Generally, a warranty is an assurance or promise regarding the existence or accuracy of facts, condition, quality, quantity or nature of a good or property. Express warranties derive from sales laws and arise when a seller makes a specific claim or assurance about a product or service that becomes part of the basis of the bargain, sale or exchange. Express warranties are often seen in the context of product sales as they cover promises regarding performance standards, quality or compliance with specifications.

Breach of implied warranty

Similar to express warranties, implied warranties have deep roots in U.S. sales law, particularly the Uniform Commercial Code, which codifies several implied warranties. Most relevant to data privacy litigation are the implied warranty of merchantability, which assures goods are fit for ordinary use, and the implied warranty of fitness for a particular purpose, which assures goods fit a buyer's specific needs. In a consumer product context, these implied warranties protect buyers against defects or misrepresentations in goods or services, even if not expressly mentioned.

Summary of breach types in the context of data breaches

TYPE OF BREACH	DEFINITION	PRIVACY INCIDENT EXAMPLE
Breach of express contract	Explicitly stated terms are violated by one party	A company explicitly promises not to share user data but does so
Breach of implied contract	Contracts are formed based on conduct or circumstances, not written terms	A company collects sensitive information, implying a duty to protect it, but fails to do so due to lax security
Breach of express warranty	Specific promises or assurances about a product/service are not met	A company advertises "zero data logging" but logs user activities, which are exposed in a data breach
Breach of implied warranty	Obligations are assumed based on the nature of the product/service, even if unstated	A cloud service implicitly promises secure storage, but data is leaked due to poor or outdated security practices

Successful strategies at preliminary stages: Unspoken promises, expected liability

Some courts have allowed breach of contract claims regarding privacy incidents to proceed past the motion to dismiss stage on the theory that employers who collect personally identifiable information as a condition of employment enter an implied contract to protect the personal information they now possess.

In 2019, Altice USA, a large media and telecommunications company, was the victim of a phishing attack through which several employees inadvertently divulged the credentials of their business email accounts. The stolen credentials were subsequently used to access and download emails and other data. In one of the accessed inboxes was a password-protected document that contained the personal information of 52,846 current and former employees.

According to the plaintiffs in McFarlane v. Altice USA, comprised of current and former employees' whose information was accessed, when Altice required them to disclose their personal information as a condition of employment, they entered an implied contract with the company to protect this data through the use of reasonable industry standards.

They further alleged examples of Altice's failure to perform its implied contractual duties included inadequate email filtering software, lack of sufficient cybersecurity training for employees with access to sensitive data, lack of encryption and the retention of personal identifying information of former employees years after they had left the company. At the motion to dismiss stage, the court agreed with the employees and the breach of implied contract claims proceeded to an eventual settlement in 2022.

This case follows the trend in some courts that emphasizes the reasonable expectations of privacy created by a company's own statements while simultaneously considering whether a reasonable consumer would interpret privacy statements as binding promises.

In In re BetterHelp Data Disclosure Cases, BetterHelp was operating a counseling service that connects customers with therapists and facilities. The company has several websites, some of which are aimed at specific groups and communities based upon religion, marital status, age, and sexual identity or orientation. At some point, BetterHelp delegated significant decision-making authority for advertising through its Facebook platform to a low-level employee who was a recent college graduate with no marketing experience, no experience in safeguarding health information and little training.

As a result, BetterHelp allegedly disclosed information of its customers and potential customers to various third parties for advertising purposes and the third parties' own purposes, which effectively revealed to the third parties that the customers were seeking and/or receiving mental health treatment. This disclosure occurred despite BetterHelp's privacy assurances throughout their website and interactive forms.

The U.S. Court of Appeals for the Ninth Circuit held that the plaintiffs sufficiently identified the particular promises they contend BetterHelp made, including assurances to keep customer information confidential, and facts that would constitute a breach of those promises. As such, the plaintiffs' breach of implied contract claim was allowed to proceed.

Decisions turn on the terms

The survival of a plaintiff's breach of contract claim will always turn on the specific language of the relevant statement, as well as the circumstances in which the defendant's breach allegedly occurred. Furthermore, even in courts that have determined a privacy notice can form an express contract, limitations within those policies can still preclude claims.

In Bass v. Facebook, multiple plaintiffs filed a data breach putative class-action lawsuit against Facebook in 2019. The plaintiffs claimed hackers exploited a coding vulnerability and stole the access tokens, which are "electronic object(s) embedded with all of a users' security information," of 69,000 users. These tokens were designed never to expire and allowed the information of connected users to be viewed. As a result, the stolen tokens of 69,000 users led to the theft of information from 29 million worldwide users.

Lawsuits claiming breach of contract and breach of implied contract, among other causes of action, were filed against Facebook. In its order on Facebook's motion to dismiss, the lower court determined, for the plaintiff with standing, that Facebook's data use policy and terms of service were construed as contractual promises to limit data sharing, and the plaintiff properly alleged such contractual promise was violated. However, the plaintiff's breach of contract claims ultimately failed because Facebook's terms of service included an accessible, procedurally fair and sufficiently clear limitation-of-liability clause.

Unsuccessful and unresolved strategies: No terms, no triumph

Breach of contract claims are often dismissed due to lack of specific, enforceable promises. In Anibal Rodriguez, et al. v. Google, the plaintiffs argued Google created a unilateral contract by providing a button to adjust a user's privacy settings. They asserted toggling the button to turn off web and app activity created a unilateral contract with Google and, accordingly, Google would not collect their data.

The district court determined providing a button for consumers to choose whether data related to their activities was saved to their accounts was insufficient to give rise to an enforceable contract. The court held that, although the button might create an expectation among users that data will not be collected, such action was not negotiated or bargained for terms in the manner contracts require and Google did not offer or receive anything in exchange for a user turning off the button.

Additionally, some plaintiffs failed to adequately counter defenses, such as sufficient disclosures. In In re Google Gmail Litig., at the pleading stage, the district court declined to certify a punitive class. The plaintiffs alleged Google routed all emails received by Gmail users through a device from which

Google acquired message content and other information used to create metadata and annotations on users. Yet the court held that, due to Google's disclosures about these alleged interceptions from a "panoply of sources," the plaintiffs could have learned of the alleged interceptions and therefore had implicitly consented.

Vague loses the day

Regarding warranty claims, many complaints have been dismissed for either lack of specificity or because privacy notices are not typically seen as warranties. When examining the counts for breach of express warranty in In re Google Assistant Privacy Litigation, the court determined the plaintiffs had not identified terms of an express warranty within the provisions of the privacy notice. Additionally, service agreements often include disclaimers that negate implied warranties, which courts have upheld. In the same case, which included the disclaimer, "to the extent permitted by law, we exclude all warranties" within the defendant's terms of service, the court upheld the disclaimers as a defense against the allegations of implied warranties.

Every word counts

Although courts have found collection of sensitive information can create an implied contract that imposes obligations on organizations, courts have also dismissed breach of contract claims when organizations have included clear limitation-of-liability clauses within their terms of service. This range of findings in the preliminary stages of cases suggests, as privacy incidents spur more private litigation, more and more circuit splits are likely to develop. Until comprehensive legislation or controlling precedent says otherwise, privacy professionals and attorneys alike must remain mindful of the ever-growing responses and novel arguments from plaintiffs in the wake of privacy incidents and develop responses to those risks accordingly.