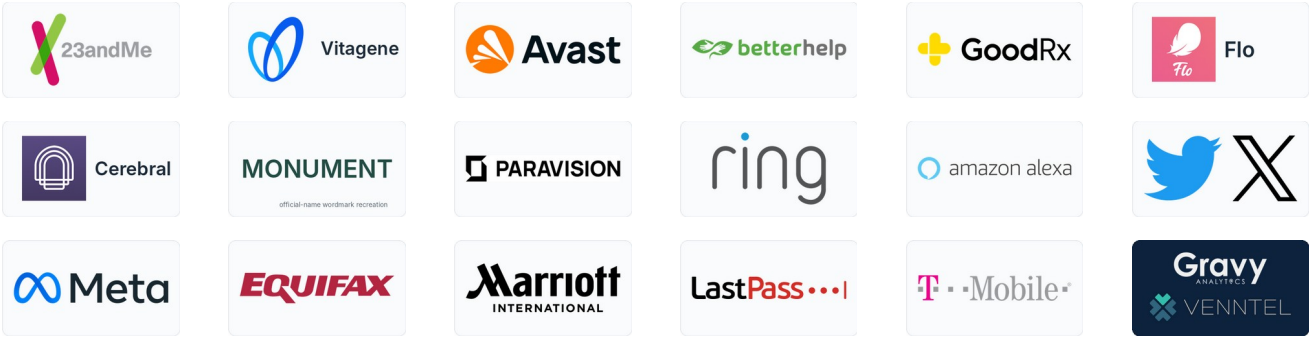
STANDALONE COMPANION RESEARCH ADDENDUM

PRIVATE DATA STEWARDSHIP FAILURES

Corporate collection, monetization, security breakdown, transfer, and downstream harm

Central proposition

Private organizations capture the economic value of collecting, retaining, combining, and transferring intimate personal information, while the costs of insecure storage, broken promises, corporate transactions, and downstream misuse are imposed primarily on the people described by the data.



18 case studies | 8 failure categories | security, health, genetics, advertising, biometrics, acquisitions, bankruptcy, and public-sector access

July 2026

SCOPE

A separate companion - not another company tier

This volume broadens the narrative beyond government-facing surveillance vendors without claiming that every case falls within the proposed GISA or Public Power Through Private Infrastructure Act.

Why it is separate

The two proposed acts focus on government information stewardship and private infrastructure deliberately supplying public investigative power. This addendum documents a wider commercial pattern: sensitive consumer data can be accumulated, monetized, exposed, inherited, auctioned, or retained in derived form even when a government actor is absent.

What inclusion means

- A company is included because an official regulator, court filing, enforcement order, or company transaction record supplies a useful public case study.
- Inclusion is not a claim that every company committed every category of conduct, or that every allegation was admitted. Many enforcement matters were resolved by settlement.
- The report separates alleged or found conduct from the broader policy inference drawn from the case.
- The unifying claim concerns incentives and stewardship, not a single conspiracy or a single class of actor.

Defensible website language

Recommended formulation

The companies and incidents documented here involve different technologies and different forms of alleged or established failure. Together, they reveal a common structural problem: organizations are rewarded for collecting, retaining, combining, and transferring personal information, while the cost of insecure storage, broken promises, corporate transfers, and downstream misuse is imposed primarily on the people described by the data.

EXECUTIVE SUMMARY

The economic value is concentrated; the risk is distributed

The cases in this report are not interchangeable. Some involve hackers. Some involve advertising pixels. Some involve product telemetry, facial recognition, inherited systems, bankruptcy, or commercial location markets. The point is that each failure occurs inside the same information economy: data is cheap to copy, valuable to retain, useful for secondary purposes, and difficult for an individual to recover once it leaves the original context.

18	8	5	1
case studies	failure categories	stages in the lifecycle	recurring accountability gap

Three observations recur

Sensitivity is not self-enforcing. Genetic, biometric, health, location, security, and identity data often receive stronger marketing language than operational protection.

Deletion is a graph problem. Backups, third-party copies, transcripts, models, embeddings, audience lists, and inferred profiles can survive the deletion of the user-facing record.

Corporate continuity can exceed user consent. Data can survive mergers, acquisitions, bankruptcy, vendor changes, and business-model shifts even though the user evaluated only the original company and purpose.

NARRATIVE FRAMEWORK

The five-stage private-data cycle

1

Data accumulation

Genetics, health, location, biometrics, communications, identity, browsing, and social relationships are collected because they improve a service or create future optionality.

2

Monetization and purpose expansion

Information is shared with advertising and analytics platforms, used to train systems, combined with outside datasets, or repurposed after a policy or business-model change.

3

Weak stewardship

Authentication, access control, monitoring, encryption, segmentation, inventory, retention, and deletion fail to match the sensitivity and scale of the information.

4

Corporate transfer

Data and obligations pass through merger, acquisition, bankruptcy, asset sale, outsourcing, cloud migration, or product shutdown.

5

Externalized harm

Consumers bear identity theft, stigma, discrimination, surveillance, familial exposure, permanent biometric compromise, or loss of control, while the commercial upside was captured elsewhere.

CLASSIFICATION

Eight failure categories

The categories are analytical labels, not legal conclusions. A case may occupy several categories at once.

Code	Category	Working definition
SF	**Security failure**	A company retained sensitive information without security proportionate to its sensitivity, permanence, scale, or connected-account exposure.
BP	**Broken privacy promise**	Representations about confidentiality, deletion, limited use, or user control materially diverged from the conduct alleged or found by regulators.
PE	**Purpose expansion**	Information collected for one reason was later used for advertising, analytics, algorithm development, or another materially different purpose.
DB	**Data brokerage / commercial sharing**	Information was sold, licensed, transferred, or disclosed into a third-party commercial ecosystem, including advertising and analytics platforms.
AR	**Acquisition risk**	An acquirer inherited sensitive information, legacy systems, or obligations that users did not necessarily evaluate when they supplied the data.
BR	**Bankruptcy risk**	Sensitive information entered a bankruptcy or asset-sale process in which privacy restrictions had to compete with creditor and transaction interests.
DR	**Derived-data retention**	Deletion of source data did not automatically eliminate backups, transcripts, embeddings, models, algorithms, or other products derived from it.
GA	**Government-access risk**	A commercial dataset or service was designed, sold, or made available for public-sector, law-enforcement, or national-security use.

CASE MAP

How the stories fit the categories

A filled cell means the category is materially useful to explaining the case; it does not imply identical severity or legal posture.

Company	SF	BP	PE	DB	AR	BR	DR	GA
23andMe	●				●	●		
1Health.io / Vitagene	●	●	●				●	
Avast / Jumpshot		●	●	●			●	
BetterHelp		●	●	●				
GoodRx		●	●	●				
Flo Health		●	●	●				
Cerebral	●	●	●	●				
Monument		●	●	●				
Everalbum / Paravision		●	●				●	
Ring	●	●	●		●		●	
Amazon Alexa		●	●				●	
Twitter (now X)		●	●					
Meta / Facebook / Cambridge Analytica		●	●	●			●	
Equifax	●							
Marriott / Starwood	●				●			
LastPass	●						●	
T-Mobile	●							
Gravy Analytics / Venntel			●	●				●

Category key: SF security failure; BP broken promise; PE purpose expansion; DB data brokerage/commercial sharing; AR acquisition risk; BR bankruptcy risk; DR derived-data retention; GA government-access risk.

CASE STUDY 01

23andMe

SF Security failure | **AR Acquisition risk** | **BR Bankruptcy risk**

DATA AT ISSUE

Genetic data, health reports, ancestry information, relatives, family trees, dates of birth, and demographic attributes.

The story

A 2023 credential-stuffing campaign directly entered a comparatively small set of accounts, but connected DNA Relatives and family features amplified the exposure across almost seven million people worldwide. UK and Canadian regulators found inadequate authentication, monitoring, and safeguards for exceptionally sensitive genetic information. In March 2025, 23andMe entered Chapter 11, placing the company and its data assets into a sale process. The business was ultimately acquired by the nonprofit TTAM Research Institute, founded by 23andMe co-founder Anne Wojcicki.

Why it fits the framework

This is the clearest example of security failure merging with corporate-transfer risk. The important claim is not that TTAM has been shown to misuse the data. It is that immutable genetic and familial information entered bankruptcy and required regulators, courts, and the purchaser to negotiate continuity of privacy protections after users had already surrendered the data.

Regulatory or transaction outcome

The UK ICO imposed a £2.31 million penalty. Canadian and UK regulators issued findings and intervened around bankruptcy protections. TTAM announced completion of the acquisition on July 14, 2025.

Primary sources

- UK ICO, 23andMe fined for failing to protect genetic data (June 17, 2025)
- Office of the Privacy Commissioner of Canada, investigation findings and impact
- Canada/UK privacy authorities, bankruptcy-protection letter
- TTAM Research Institute, acquisition completion announcement

CASE STUDY 02

1Health.io / Vitagene

SF Security failure **BP Broken privacy promise** **PE Purpose expansion** **DR Derived-data retention**

DATA AT ISSUE

DNA test results, genetic information, health information, customer identities, and biological samples.

The story

The FTC alleged that Vitagene, later renamed 1Health.io, promised strong protection for highly personal DNA information while leaving unencrypted health and genetic data in publicly accessible cloud-storage buckets. The company allegedly received repeated warnings. The FTC also challenged a retroactive privacy-policy change that expanded how customer data could be shared and alleged failures to honor deletion commitments.

Why it fits the framework

The case links cybersecurity to the integrity of privacy promises. A privacy policy is not meaningful if the technical system exposes the data or if the company can later rewrite the purpose of collection. It also demonstrates that genetic stewardship may include both digital records and physical samples.

Regulatory or transaction outcome

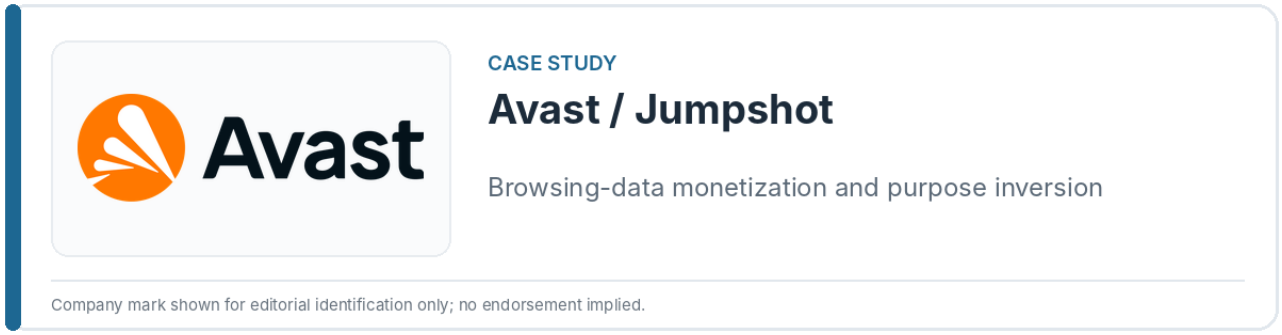
The FTC finalized an order requiring a privacy and security program, deletion or destruction obligations, limits on retroactive policy changes, and $75,000 for consumer refunds.

Primary sources

- FTC, genetic testing company failed to protect DNA data and changed privacy policy
- FTC, final order with 1Health.io

CASE STUDY 03

Avast / Jumpshot



BP Broken privacy promise	PE Purpose expansion	DB Data brokerage / commercial sharing	DR Derived-data retention

DATA AT ISSUE

Granular web-browsing histories collected through antivirus software and browser extensions.

The story

The FTC alleged that Avast promoted products as protecting people from online tracking while collecting detailed browsing information and transferring it to its Jumpshot subsidiary. Jumpshot sold information to more than 100 third parties, and the FTC described the data as sufficiently detailed to create re-identification risks. The data was stored indefinitely without adequate notice or consent, according to the complaint.

Why it fits the framework

This is a direct inversion of the product promise: privacy protection became a collection channel. It shows how data gathered under a security rationale can be converted into a commercial intelligence product and how derived products or algorithms can preserve value after the raw dataset is withdrawn.

Regulatory or transaction outcome

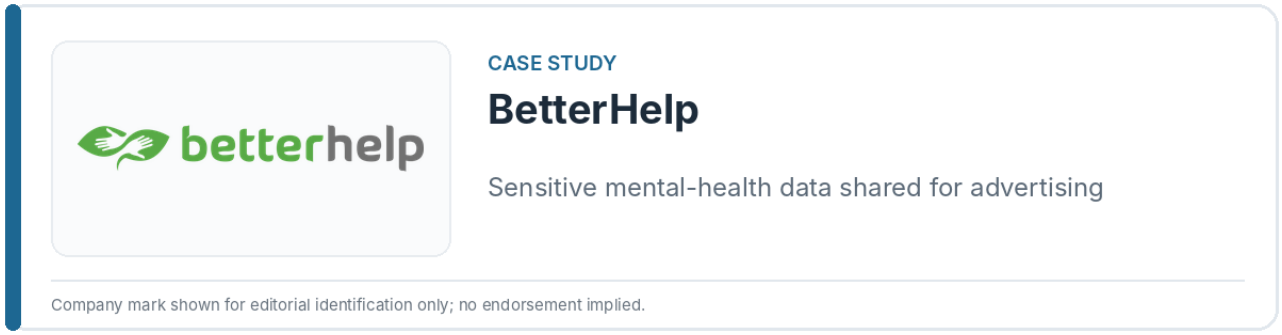
Avast agreed to pay $16.5 million. The final FTC order bans specified sales and requires deletion of transferred browsing data and products or algorithms derived from it.

Primary sources

- FTC, final Avast order
- FTC, Avast refund process and Jumpshot sales allegations

CASE STUDY 04

BetterHelp



BP Broken privacy promise | **PE Purpose expansion** | **DB Data brokerage / commercial sharing**

DATA AT ISSUE

Email and IP addresses, therapy enrollment, mental-health questionnaire responses, and related personal information.

The story

The FTC alleged that BetterHelp promised limited and confidential use of sensitive information but disclosed email addresses, IP addresses, and health-questionnaire information to advertising platforms including Facebook, Snapchat, Criteo, and Pinterest. The disclosures were used for advertising and retargeting even though consumers approached the service in a mental-health context.

Why it fits the framework

The case illustrates why nominally pseudonymous advertising identifiers are not harmless when attached to the fact that someone sought therapy or disclosed a condition. Commercial optimization displaced the contextual expectation that information given to obtain counseling would remain within the care relationship.

Regulatory or transaction outcome

The FTC finalized a $7.8 million order, banned health-data sharing for advertising, required affirmative consent for specified disclosures, ordered deletion instructions to recipients, and imposed a retention schedule.

Primary sources

- FTC, final BetterHelp order

CASE STUDY 05

GoodRx

BP Broken privacy promise | **PE Purpose expansion** | **DB Data brokerage / commercial sharing**

DATA AT ISSUE

Prescription medications, health conditions, contact details, device identifiers, and coupon or service activity.

The story

The FTC alleged that GoodRx repeatedly promised not to share personal health information with advertisers or third parties but sent prescription and health information to Facebook, Google, Criteo, and others. It also allegedly used customer lists and health information to target users with medication- and condition-specific advertisements.

Why it fits the framework

GoodRx shows how a consumer health service can become part of an advertising supply chain without the user experiencing an obvious "sale." APIs, pixels, custom audiences, and analytics integrations can turn service activity into commercial targeting data while remaining largely invisible to the person described.

Regulatory or transaction outcome

GoodRx agreed to a $1.5 million civil penalty in the FTC's first Health Breach Notification Rule enforcement action, along with advertising restrictions, consent requirements, deletion directions, and a public retention schedule.

Primary sources

- FTC, GoodRx health-data enforcement action

CASE STUDY 06

Flo Health

BP Broken privacy promise | **PE Purpose expansion** | **DB Data brokerage / commercial sharing**

DATA AT ISSUE

Menstrual-cycle, fertility, pregnancy, and other reproductive-health activity recorded through the app.

The story

The FTC alleged that Flo promised to keep users' health information private and use it to provide the service, but transmitted sensitive app events to marketing and analytics providers including Facebook and Google. Some events could disclose facts such as pregnancy. The FTC said Flo did not adequately limit how recipients could use the information.

Why it fits the framework

The case demonstrates that technical event labels can carry intimate meaning even when a dataset does not look like a medical chart. Product telemetry and analytics can effectively disclose pregnancy, fertility, or sexual-health context and thereby expand a care-oriented purpose into advertising and measurement.

Regulatory or transaction outcome

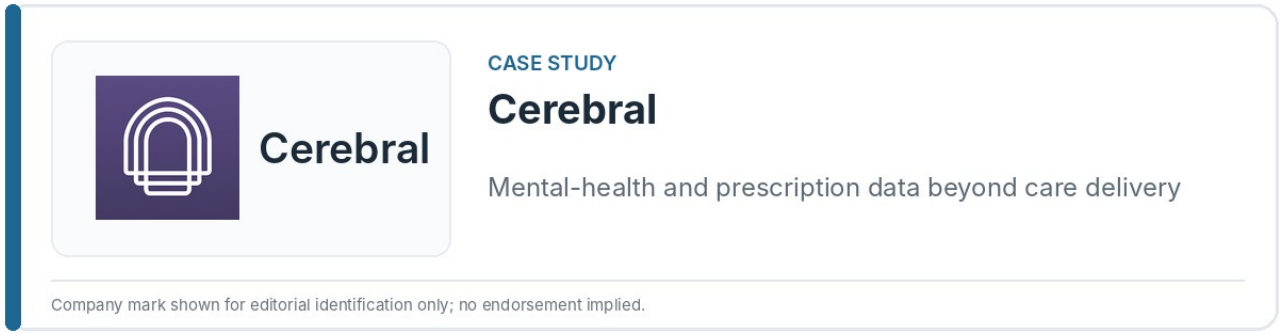
The FTC finalized an order requiring affirmative consent, notification to affected users, deletion instructions to third parties, and an independent privacy review.

Primary sources

- FTC, final Flo Health order
- FTC, original Flo Health complaint announcement

CASE STUDY 07

Cerebral



SF Security failure | **BP Broken privacy promise** | **PE Purpose expansion** | **DB Data brokerage / commercial sharing**

DATA AT ISSUE

Mental-health and prescription histories, treatment plans, insurance and pharmacy data, identity documents, beliefs, and other sensitive profile information.

The story

The FTC alleged that Cerebral marketed its telehealth service as safe, secure, and discreet while disclosing sensitive information to advertising and social-media platforms through tracking technologies. The complaint described nearly 3.2 million consumers and also alleged weak access controls and other security practices.

Why it fits the framework

Cerebral shows that the same organizational incentives can produce both disclosure and security failures. A company that collects broad clinical and identity information can increase marketing performance by exposing data to external platforms while simultaneously increasing the consequences of weak internal stewardship.

Regulatory or transaction outcome

The proposed federal order included more than $7 million in payments, restrictions on advertising uses, consent and deletion requirements, a comprehensive privacy and security program, and a retention schedule.

Primary sources

- FTC, proposed Cerebral order

CASE STUDY 08

Monument

MONUMENT

official-name wordmark recreation

CASE STUDY

Monument

Addiction-treatment data shared for advertising

Company mark shown for editorial identification only; no endorsement implied.

BP Broken privacy promise	PE Purpose expansion	DB Data brokerage / commercial sharing

DATA AT ISSUE

The fact of seeking alcohol-addiction treatment, therapy and medication activity, email addresses, IP addresses, and service interactions.

The story

The FTC alleged that Monument disclosed sensitive health information to Meta and Google through advertising technologies after promising confidentiality. The shared information could reveal that a specific person was receiving help for alcohol addiction, including therapy or medication-related services.

Why it fits the framework

The case makes the externalized-harm problem unusually clear. Advertising systems receive commercial value, while the user bears potential stigma, embarrassment, employment, housing, insurance, and emotional consequences. The harm does not depend on publication to the general public; it begins with uncontrolled entry into a commercial network.

Regulatory or transaction outcome

The settlement bans health-data disclosure for advertising, requires affirmative consent for other specified sharing, and imposes privacy and security obligations. A $2.5 million civil penalty was suspended based on ability to pay.

Primary sources

- FTC, Monument enforcement announcement
- FTC, Monument complaint

CASE STUDY 09

Everalbum / Paravision

BP Broken privacy promise | **PE Purpose expansion** | **DR Derived-data retention**

DATA AT ISSUE

Personal photos and videos, facial embeddings, facial-recognition models, and content retained after account deactivation.

The story

The FTC alleged that the Ever photo-storage app misrepresented when facial recognition would be enabled and retained photos and videos from users who had deactivated their accounts. Those images were used to develop face-recognition technology that later became associated with the Paravision business.

Why it fits the framework

This is a model case for derived-data stewardship. Deleting or closing an account is incomplete if the company retains face embeddings, training examples, models, or algorithms created from the user's material. The commercial product may outlive the source relationship and preserve the benefit of conduct regulators found deceptive.

Regulatory or transaction outcome

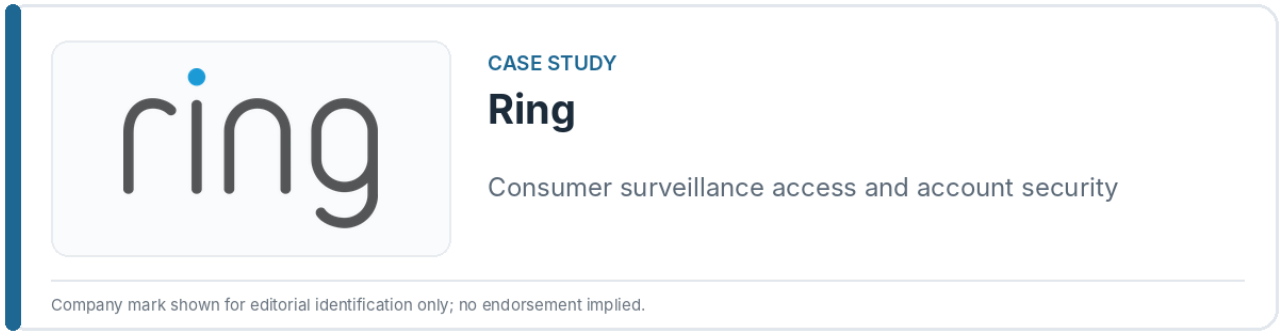
The FTC order required express consent for facial recognition and deletion of affected photos, videos, face embeddings, and models or algorithms developed from improperly retained or used data.

Primary sources

- FTC, final Everalbum settlement
- FTC, Everalbum order

CASE STUDY 10

Ring



SF Security failure	BP Broken privacy promise	PE Purpose expansion	AR Acquisition risk	DR Derived-data retention

DATA AT ISSUE

Private home-security video, camera account data, face embeddings, and work products derived from customer recordings.

The story

The FTC alleged that Ring allowed overly broad employee and contractor access to customer videos, used videos for algorithm development without adequate consent, and failed to implement protections that could have reduced credential-stuffing attacks. Hackers gained control of some accounts, cameras, and videos. Amazon acquired Ring in 2018.

Why it fits the framework

Ring joins acquisition, intimate home surveillance, algorithm development, and weak access governance. It demonstrates why a company's internal workforce, contractors, acquirer, and model-development teams all belong within the stewardship chain. A camera sold for household security can produce a long-lived training asset.

Regulatory or transaction outcome

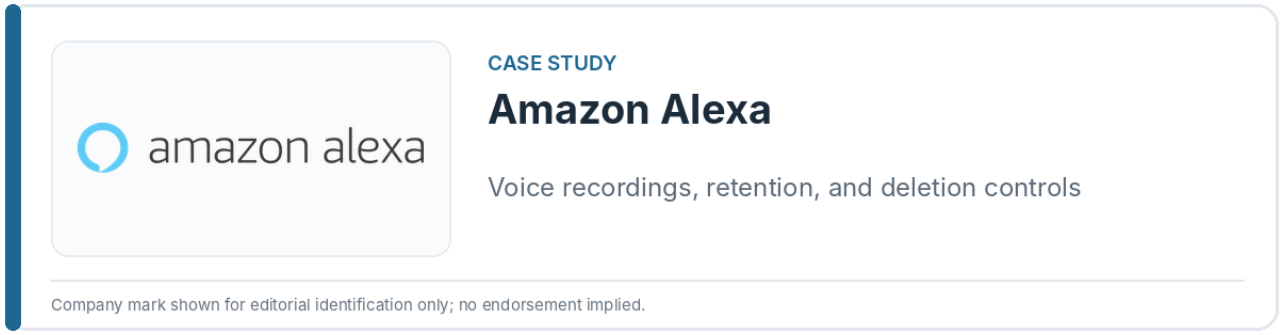
Ring agreed to pay $5.8 million and implement a privacy and security program. The order required deletion of specified pre-2018 videos, face embeddings, and derived work products.

Primary sources

- FTC, Ring enforcement announcement
- FTC, Ring refunds

CASE STUDY 11

Amazon Alexa



BP Broken privacy promise | **PE Purpose expansion** | **DR Derived-data retention**

DATA AT ISSUE

Children's and adults' voice recordings and transcripts, geolocation data, account activity, and algorithm-training material.

The story

The FTC and DOJ alleged that Amazon retained children's Alexa voice recordings indefinitely unless a parent requested deletion and, even after deletion requests, failed to remove some transcripts from all databases. The complaint also challenged geolocation deletion practices. Retained recordings were valuable for improving speech-recognition and processing systems.

Why it fits the framework

Alexa demonstrates how "deletion" can fail across databases and how retained data can continue producing algorithmic value. A company may stop displaying a recording to the user while still retaining transcripts or using the material to improve a product, leaving the user's request ineffective at the descendant-data level.

Regulatory or transaction outcome

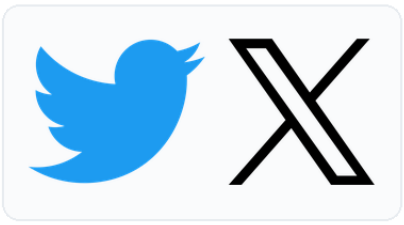
Amazon agreed to a $25 million civil penalty, revised deletion practices, privacy safeguards, and prohibitions on using data subject to deletion requests to create or improve data products.

Primary sources

- FTC/DOJ, Amazon Alexa children's privacy action
- FTC, Amazon Alexa case summary

CASE STUDY 12

Twitter (now X)



CASE STUDY

Twitter (now X)

Security failures and deceptive account-security representations

Company mark shown for editorial identification only; no endorsement implied.

BP Broken privacy promise **PE Purpose expansion**

DATA AT ISSUE

Phone numbers and email addresses supplied for account security, two-factor authentication, and account recovery.

The story

The FTC and DOJ charged Twitter with using contact information collected for security to support targeted advertising. Users were asked to provide phone numbers or email addresses to protect or recover accounts, but the company also allowed advertisers to use the data for targeting from 2014 through 2019.

Why it fits the framework

The case is a concise example of purpose incompatibility. Security data is often mandatory or strongly encouraged because the platform frames it as protection. Reusing it for advertising converts a trust and safety control into a revenue input and may discourage users from adopting stronger authentication.

Regulatory or transaction outcome

Twitter agreed to pay a $150 million penalty and was prohibited from profiting from deceptively collected security data, along with compliance and user-notice obligations.

Primary sources

- FTC, Twitter account-security data enforcement

CASE STUDY 13

Meta / Facebook / Cambridge Analytica

BP Broken privacy promise | **PE** Purpose expansion | **DB** Data brokerage / commercial sharing | **DR** Derived-data retention

DATA AT ISSUE

Social profiles, friend-network information, app permissions, interests, political and behavioral profiles, and advertising identifiers.

The story

The FTC alleged that Facebook undermined users' privacy choices and allowed third-party applications broad access to personal information. The Cambridge Analytica matter involved data collected through an app and used to build voter-profiling and targeting capabilities. The FTC separately brought actions against Facebook, Cambridge Analytica, its former CEO, and the app developer.

Why it fits the framework

This ecosystem illustrates how a platform can monetize data while distributing collection and responsibility across developers, analytics firms, advertisers, and political customers. Even after source access is cut off, copied datasets, inferred traits, audiences, and models can remain valuable and difficult to audit or delete.

Regulatory or transaction outcome

Facebook agreed to a $5 billion penalty and a 20-year privacy-governance order. The FTC issued a final order against Cambridge Analytica and settlements requiring deletion and restrictions for associated individuals.

Primary sources

- FTC, Facebook $5 billion privacy order
- FTC, Cambridge Analytica action
- FTC, Cambridge Analytica case timeline

CASE STUDY 14

Equifax

SF Security failure

DATA AT ISSUE

Names, Social Security numbers, dates of birth, addresses, credit information, and some payment-card and identity-document data.

The story

The 2017 Equifax breach exposed personal information associated with approximately 147 million people. Regulators alleged that the credit-reporting company failed to take reasonable steps to secure its network. Unlike many consumer services, people generally cannot avoid being described in a credit bureau's databases simply by declining to create an account.

Why it fits the framework

Equifax demonstrates involuntary data custody and externalized risk. The company's business depends on consolidating identity and financial information, but the individuals bear the long-term burden of fraud monitoring and identity exposure. Social Security numbers and birth dates cannot be meaningfully rotated like passwords.

Regulatory or transaction outcome

Equifax agreed to pay at least $575 million, potentially up to $700 million, in a global settlement with the FTC, CFPB, states, and territories, including consumer assistance and security requirements.

Primary sources

- FTC, Equifax settlement announcement
- FTC, Equifax settlement information

CASE STUDY 15

Marriott / Starwood

SF Security failure **AR Acquisition risk**

DATA AT ISSUE

Passport information, payment-card data, loyalty numbers, dates of birth, email addresses, reservation records, and other guest information.

The story

The FTC alleged that security failures at Marriott and Starwood contributed to three breaches affecting more than 344 million customers worldwide. The Starwood intrusion began before Marriott completed its acquisition, making the matter a prominent example of inherited cyber risk and the difficulty of integrating legacy systems and data estates.

Why it fits the framework

A merger transfers more than revenue and customers. It transfers historical databases, security debt, vendor relationships, and latent compromise. Acquisition diligence that focuses on financial assets without validating data inventory, access, encryption, logging, and breach history can shift the consequences to guests.

Regulatory or transaction outcome

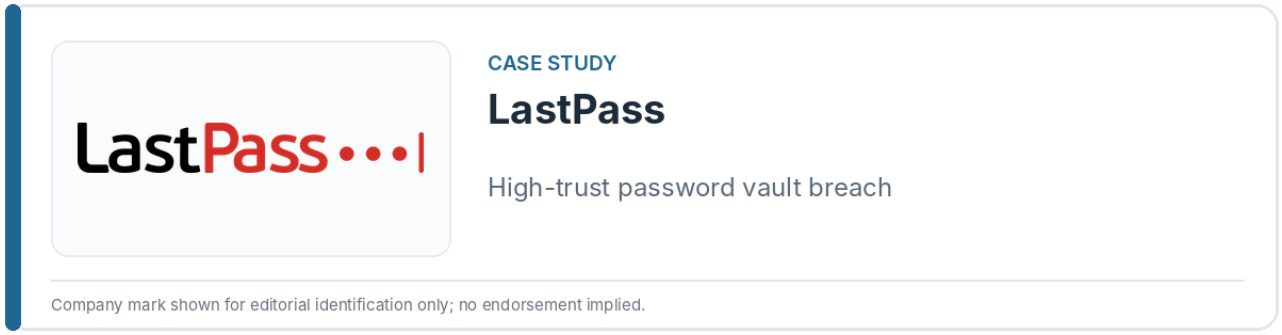
The FTC finalized an order requiring a comprehensive information-security program, data-retention limits, and a deletion-request mechanism. Marriott also reached a parallel settlement with state attorneys general.

Primary sources

- FTC, Marriott and Starwood breach action
- FTC, final Marriott and Starwood order

CASE STUDY 16

LastPass



SF Security failure **DR Derived-data retention**

DATA AT ISSUE

Customer-account information and encrypted password-vault backup data held by a high-trust password-management provider.

The story

The UK ICO found that LastPass failed to implement sufficiently robust technical and organizational measures, enabling a threat actor to exfiltrate personal data relating to approximately 1.6 million UK customers from a backup database in the 2022 incident. The ICO stated that there was no evidence customer vault passwords were decrypted.

Why it fits the framework

LastPass demonstrates that backups are not passive insurance copies; they are active concentrations of risk. A high-trust custodian may advertise security as its core value, yet an inadequately protected backup can preserve a historical and highly attractive dataset outside the primary system's normal controls.

Regulatory or transaction outcome

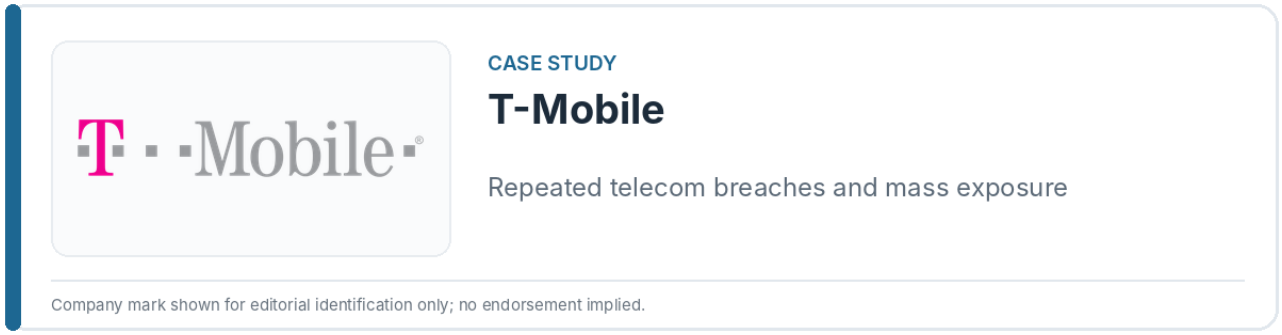
The ICO issued a £1,228,283 penalty in November 2025. The case emphasizes security architecture, backup protection, monitoring, and the heightened duty associated with password-management services.

Primary sources

- UK ICO, LastPass fine announcement
- UK ICO, LastPass enforcement record

CASE STUDY 17

T-Mobile



SF Security failure

DATA AT ISSUE

Subscriber identity, account, contact, telecommunications, and related customer information affected across multiple incidents.

The story

The FCC investigated significant T-Mobile breaches in 2021, 2022, and 2023 that affected millions of U.S. consumers. The settlement focused not only on a single intrusion but on foundational security controls, cyber hygiene, modern architecture, and phishing-resistant authentication.

Why it fits the framework

Repeated incidents show why breach disclosure alone does not establish stewardship. A company with recurring access to large customer populations must demonstrate systemic remediation rather than treating each breach as an isolated event. Scale turns ordinary weaknesses into national exposure.

Regulatory or transaction outcome

T-Mobile agreed to a $15.75 million civil penalty and an additional $15.75 million investment in cybersecurity improvements, including zero-trust and phishing-resistant multifactor-authentication commitments.

Primary sources

- FCC, T-Mobile breach settlement press release

CASE STUDY 18

Gravy Analytics / Venntel

CASE STUDY

Gravy Analytics / Venntel

Location-data brokerage, government sales, and breach risk

Company mark shown for editorial identification only; no endorsement implied.

PE Purpose expansion	DB Data brokerage / commercial sharing	GA Government-access risk

DATA AT ISSUE

Precise mobile-device location, movement histories, visits to sensitive locations, and commercial geolocation analytics.

The story

The FTC alleged that Gravy Analytics and its Venntel subsidiary collected, used, and sold sensitive location data, including information capable of revealing visits to health clinics, religious sites, labor organizations, military locations, and other sensitive places. Venntel's products were sold into public-sector, national-security, and law-enforcement markets.

Why it fits the framework

This case directly connects private commercial collection to public power. A consumer may disclose location to an app for an ordinary service, while intermediaries aggregate it into a retrospective tracking product. The initial collector, broker, government customer, and affected person may never have a direct relationship.

Regulatory or transaction outcome

The FTC finalized an order restricting the sale, disclosure, and use of sensitive location data, subject to limited law-enforcement and national-security circumstances, and requiring a sensitive-location data program.

Primary sources

- FTC, final Gravy Analytics and Venntel order
- FTC, original Gravy Analytics and Venntel action

CROSS-CASE FINDINGS

What becomes visible when the cases are read together

1

The collection decision is the original risk decision

Once immutable or high-stakes data is collected, every later security, vendor, litigation, bankruptcy, and governance problem becomes more consequential. Minimization is therefore not merely a privacy preference; it is loss prevention.

2

Connected features amplify a small entry point

23andMe's relative network, Facebook's app ecosystem, Ring's account access, and advertising-platform integrations show that exposure is often determined by graph structure rather than the count of directly compromised credentials.

3

"Sharing" is broader than a conventional sale

Pixels, software-development kits, APIs, custom audiences, analytics events, model training, and remote queries can transfer economic value and control without a contract labeled as a data sale.

4

Deletion must reach descendants

Everalbum, Alexa, Avast, Ring, and 1Health show why deletion rules should reach embeddings, models, transcripts, work products, backups, and physical samples where technically and legally appropriate.

5

Corporate transactions are privacy events

Marriott/Starwood and 23andMe show two different transaction risks: inherited technical compromise and transfer of sensitive data through bankruptcy. Privacy review should be a condition of diligence, approval, and post-closing integration.

6

The user often cannot meaningfully exit

Credit reporting, telecom service, family-linked genetics, and unavoidable advertising infrastructure weaken the assumption that market choice alone can discipline misuse.

POLICY IMPLICATIONS

A private-data stewardship framework

These ideas are independent of whether this project eventually becomes a model statute, an advocacy platform, or a public incident database.

Principle	Practical rule
Restrictions follow the data	Privacy, purpose, retention, and deletion obligations should bind successors, purchasers, bankruptcy estates, vendors, subprocessors, and recipients.
No unilateral material purpose change	A company should not obtain broader rights to sensitive data merely by rewriting a privacy policy. Material expansion should require renewed, specific consent or a distinct lawful basis.
Security proportional to permanence and sensitivity	Genetic, biometric, health, identity, location, and security-authentication information should receive stronger authentication, segmentation, monitoring, and access-review requirements.
Transaction-level privacy diligence	Mergers, asset sales, and bankruptcy transfers involving sensitive datasets should require inventory, security validation, successor commitments, deletion options, and independent review.
Graph-aware deletion	Deletion should address copies, recipients, backups, indexes, embeddings, transcripts, audience lists, models, and samples, with transparent exceptions for technical impossibility and legal holds.
Commercial-sharing transparency	Companies should identify categories of recipients, purposes, data fields, and downstream uses rather than hiding material flows behind labels such as analytics or service provider.
Rights against downstream use	People should be able to obtain an accounting, dispute inaccurate profiles, and prevent materially adverse decisions based solely on opaque derived data.
Enforcement tied to data-derived benefit	Remedies may need to remove not only unlawful source data but also the commercial advantage, models, or products derived from it.

WEBSITE APPLICATION

How to tell the story without overstating it

Recommended navigation

- **The data economy:** Explain why intimate information is accumulated and how the commercial upside is created.
- **Failure categories:** Let visitors filter cases by security, promise, purpose, brokerage, acquisition, bankruptcy, derived data, or government access.
- **Company case studies:** Present one sourced narrative per company with date, data type, conduct, outcome, and category tags.
- **The transfer problem:** Create a dedicated visual path from original user consent through vendors, acquirers, bankruptcy, models, and public-sector customers.
- **Policy responses:** Connect each failure mode to a concrete legal or technical duty rather than relying on generalized outrage.

Editorial guardrails

- Use “the FTC alleged,” “the regulator found,” or “the order required” according to the source’s procedural posture.
- Do not describe a breach as a sale, or a commercial disclosure as a hack, unless the evidence supports both.
- Do not imply that an acquirer has misused inherited data merely because a transfer occurred.
- Distinguish affected accounts, directly accessed accounts, exposed profiles, and total people whose information was implicated.
- Link every numerical claim and enforcement outcome to the primary source.

Suggested section name

Private Data Stewardship Failures

METHODOLOGY AND LIMITATIONS

How this addendum was assembled

Source priority - Official enforcement releases, complaints, orders, regulator findings, court or agency documents, and first-party transaction announcements were prioritized.

Research date - Public sources were reviewed through July 25, 2026. Older incidents are included where they establish a reusable failure pattern.

Procedural posture - The report uses allegation language for complaints and settlement matters unless a regulator issued a formal finding. Settlement does not necessarily constitute an admission.

Category assignment - Categories are editorial classifications based on the public record. They are intended to support navigation and policy analysis, not establish statutory liability.

Company marks - The report reproduces company logos or official app marks solely for editorial identification; trademark rights remain with their respective owners and no endorsement is implied. Where a clean distributable official mark was not available, the report uses a clearly disclosed editorial wordmark recreation.

Scope - The case list is illustrative rather than exhaustive. It emphasizes variety across genetics, health, advertising, biometrics, identity, hospitality, telecommunications, password management, and location data.

Relationship to the two model acts

This addendum is intentionally independent. Some cases, particularly Gravy Analytics/Venntel, overlap with government-access and commercial-surveillance concerns. Others are purely private-sector examples. Their value is cumulative: they show why custody, provenance, purpose, transfer, retention, deletion, and redress should be treated as continuing obligations rather than one-time consent events.

SOURCE DIRECTORY

Primary sources by company

Hyperlinks below point to official regulators, agency documents, or first-party transaction announcements used in the case narratives.

23andMe
- UK ICO, 23andMe fined for failing to protect genetic data (June 17, 2025)
- Office of the Privacy Commissioner of Canada, investigation findings and impact
- Canada/UK privacy authorities, bankruptcy-protection letter
- TTAM Research Institute, acquisition completion announcement

1Health.io / Vitagene
- FTC, genetic testing company failed to protect DNA data and changed privacy policy
- FTC, final order with 1Health.io

Avast / Jumpshot
- FTC, final Avast order
- FTC, Avast refund process and Jumpshot sales allegations

BetterHelp
- FTC, final BetterHelp order

GoodRx
- FTC, GoodRx health-data enforcement action

Flo Health
- FTC, final Flo Health order
- FTC, original Flo Health complaint announcement

Cerebral
- FTC, proposed Cerebral order

Monument
- FTC, Monument enforcement announcement
- FTC, Monument complaint

Everalbum / Paravision
- FTC, final Everalbum settlement
- FTC, Everalbum order

Ring
- FTC, Ring enforcement announcement
- FTC, Ring refunds

Amazon Alexa
- FTC/DOJ, Amazon Alexa children's privacy action
- FTC, Amazon Alexa case summary

Twitter (now X)
- FTC, Twitter account-security data enforcement

Meta / Facebook / Cambridge Analytica

- FTC, Facebook $5 billion privacy order
- FTC, Cambridge Analytica action
- FTC, Cambridge Analytica case timeline

Equifax

- FTC, Equifax settlement announcement
- FTC, Equifax settlement information

Marriott / Starwood

- FTC, Marriott and Starwood breach action
- FTC, final Marriott and Starwood order

LastPass

- UK ICO, LastPass fine announcement
- UK ICO, LastPass enforcement record

T-Mobile

- FCC, T-Mobile breach settlement press release

Gravy Analytics / Venntel

- FTC, final Gravy Analytics and Venntel order
- FTC, original Gravy Analytics and Venntel action

CONCLUSION

Data should carry obligations, not merely value

The cases in this addendum do not tell one identical story. They show a repeated imbalance. Organizations can preserve personal data across products, vendors, advertising systems, backups, algorithms, mergers, and bankruptcy. The individual is expected to manage that expanding network through passwords, privacy policies, deletion buttons, and market choice - tools that are often structurally incapable of reaching the full data lineage.

Final proposition

A durable privacy framework should treat sensitive data as an asset burdened by continuing duties. Collection creates responsibility. Restrictions should survive copying and corporate transfer. Deletion should reach identifiable descendants. And commercial profit should not depend on shifting the cost of failure to people who cannot replace their DNA, biometrics, identity history, or private life.

Prepared as a standalone companion to the Government Information Stewardship Act and Public Power Through Private Infrastructure project.