ChatGPT

Research Justifications for Caring About Privacy Rights

Executive summary

Privacy rights are not merely about secrecy or preference. In contemporary law, policy, and technical risk management, they function as protections against coercion, discrimination, manipulation, and exposure to violence. International human rights law treats privacy as a core right connected to dignity, family life, correspondence, and reputation; EU law separately elevates personal-data protection to fundamental-right status; and children's privacy receives its own treaty protection. Research and policy work also show that privacy supports autonomy, social participation, trust in digital markets, and resistance to chilling effects produced by surveillance. [1]

The case studies below show that privacy failures regularly convert data into leverage. Ashley Madison turned intimate profile data into reputational crisis and extortion risk; Equifax turned static identifiers into long-tail fraud exposure; Vastaamo turned psychotherapy records into blackmail; SpyFone turned covert monitoring into domestic-abuse infrastructure; Grindr turned app participation into inferred sexual-orientation disclosure; Pegasus in El Salvador compromised journalists' sources and altered newsroom operations; the UK Afghan relocation leak put already-threatened people at risk of Taliban reprisals; the OPM breach created state-scale blackmail and counter-intelligence exposure; VTech exposed children's images and chats; and 23andMe showed the special danger of immutable genetic data, including data associated with racial and ethnic identity. [2]

Commercially, the strongest privacy businesses are not generic "privacy apps" sold in the abstract. The most credible opportunities sit where data is both unusually sensitive and already tied to obvious legal liability or high-consequence harms: mental-health records, consumer genomics, children's connected products, dating and LGBTQ+ platforms, high-risk communications for journalists and dissidents, anti-stalkerware services, refugee or relocation case-management, and workforce-security systems. That inference follows directly from the sectors that have already generated major enforcement actions, court cases, emergency remediation costs, or measurable distress. [3]

The business implication is straightforward. A privacy company that wants durable demand should sell **reduced attack surface, reduced coercion risk, faster redress, and higher trust**. A privacy company that wants legitimacy should avoid dark patterns, default to data minimisation, build deletion and portability that actually work, offer strong authentication and encryption where appropriate, and refuse business models built on reselling sensitive data. Regulators increasingly expect privacy by design and secure-by-design architecture, not post-incident apologetics. [4]

Why privacy rights matter

The **ethical** justification begins with autonomy and dignity. Privacy law and scholarship consistently treat privacy as part of what lets persons form relationships, deliberate, experiment, and manage the boundaries between self, family, work, politics, and intimacy. Human rights materials frame privacy as protection against arbitrary interference with private life, home, correspondence, honour, and

reputation; European human-rights doctrine protects “private life” broadly; and privacy scholarship links privacy with autonomy and human flourishing rather than with mere concealment. [5]

The **legal** justification is unusually strong because privacy is not only a policy aspiration but a recognised right. Article 12 UDHR, Article 17 ICCPR, Article 8 ECHR, Article 16 CRC, and Article 8 of the EU Charter all protect privacy or personal data in explicit terms. In the EU, personal-data protection is separately recognised as a fundamental right, not merely a derivative of consumer law. That matters commercially because products serving EU and UK users are entering a rights-based regulatory environment, not a purely contractual one. [6]

The **economic** justification is that privacy is part of the trust infrastructure of digital markets. OECD work states that respect for privacy is essential to a well-functioning digital economy because confidence in data protections increases willingness to participate online. Economic research likewise treats privacy as a domain of trade-offs, asymmetries, and market failures, especially where people cannot realistically understand, compare, or negotiate how their data will be used. In other words, privacy is not the enemy of markets; it is a condition for markets that users can rationally trust. [7]

The **social and democratic** justification is that surveillance and exposure change behaviour before any final punishment occurs. OHCHR’s 2026 study documents serious chilling effects from contemporary surveillance ecosystems, and newer causal research finds that dataveillance can induce self-censorship in ordinary digital communication. For journalists, activists, and political dissidents, privacy is therefore intertwined with freedom of expression, association, and source protection. The El Faro case is not an exception to this principle; it is an unusually well-documented illustration of it. [8]

The **safety-based** justification is the least abstract. NIST’s privacy engineering work treats privacy risk as something that can produce concrete harm and therefore requires system design choices, not just notice text. CISA now explicitly recommends end-to-end encrypted communications for highly targeted persons, while governments that often disagree on lawful access still acknowledge that strong encryption plays a crucial role in protecting personal data, cyber security, journalists, and vulnerable people in repressive contexts. The real-world cases below show why: privacy loss can become stalking, extortion, identity theft, blackmail, retaliation, discrimination, or lethal targeting. [9]

Comparative map of harms and opportunities

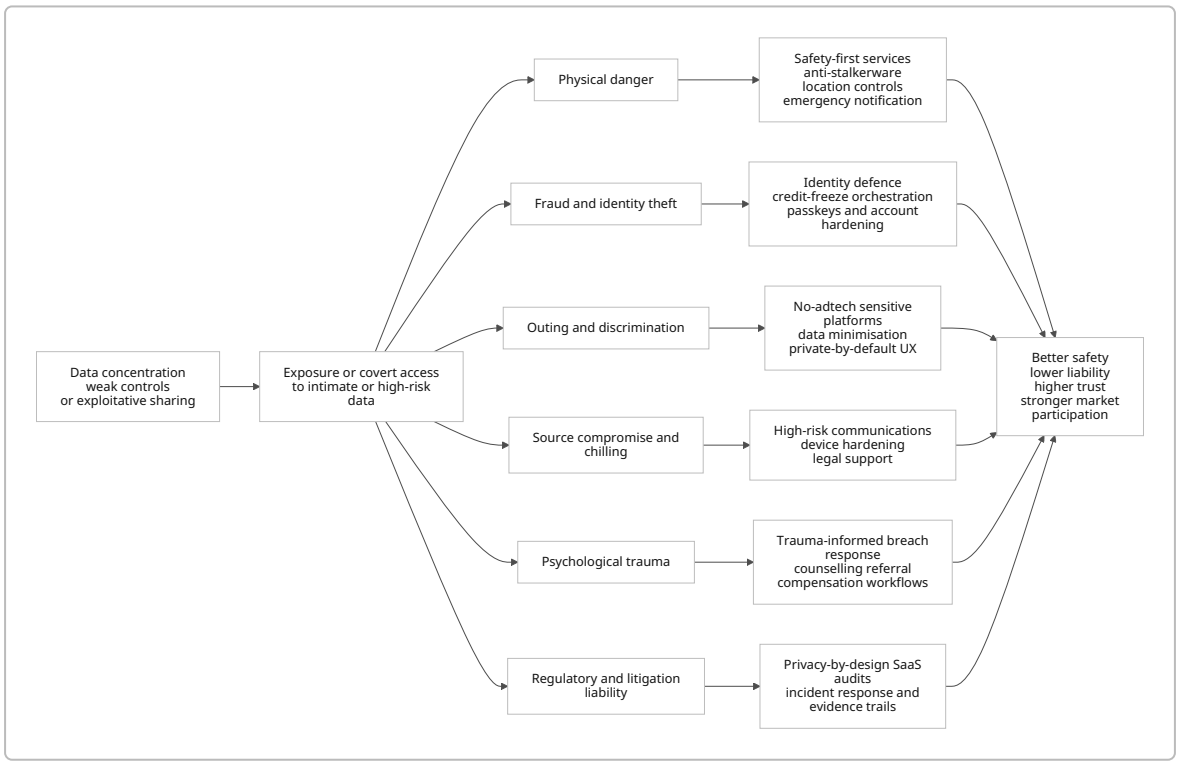
The comparative pattern is consistent across jurisdictions: **data concentration + weak controls or exploitative sharing + high-sensitivity context = outsized human harm**. The commercially important corollary is that privacy products work best when they are anchored to a concrete workflow rather than sold as vague virtue.

Case	Jurisdiction	Primary affected group	Data exposed or misused	Best-fit service or product	Likely payer and revenue model	Core sources
Ashley Madison	Canada, Australia, US, global	Ordinary adults, some non-users falsely linked	Intimate profiles, emails, profile text, deleted-account residue	Alias/relay identity, verified deletion, intimate-data minimisation	Dating platforms; B2B SaaS + compliance retainers	[10]

Case	Jurisdiction	Primary affected group	Data exposed or misused	Best-fit service or product	Likely payer and revenue model	Core sources
Equifax	US, UK, Canada	Ordinary consumers	Names, DOBs, SSNs, cards, credit data	Credit-freeze orchestration, identity wallet, breach-response concierge	Banks, insurers, employers; B2B2C subscription	11
Vastaamo	Finland	Therapy patients	Psychotherapy records, notes, identifiers	Encrypted EHR segmentation, patient breach-support platform	Clinics, EHR vendors, insurers; enterprise SaaS + managed service	12
SpyFone	US, global	Domestic-abuse survivors, monitored workers, children	GPS, messages, photos, web history, app activity	Anti-stalkerware tooling, safe-device replacement, survivor workflow	Carriers, NGOs, insurers, family-safety orgs; subscription + grant/B2B	13
Grindr	Norway, UK, US, EU/ EEA	LGBTQ+ users	App identity plus user data shared into adtech ecosystem, implying sexual orientation	Sensitive-platform privacy SDK, no-adtech mode, coarse location defaults	Dating/social apps; SDK licensing + premium subscriptions	14
Pegasus against El Faro	El Salvador, US litigation context	Journalists, activists, political dissidents	Full-device compromise, communications, sources, activities	High-risk mobile defence, secure newsroom ops, spyware-response retainer	Newsrooms, NGOs, philanthropy, diplomatic security buyers	15
Afghan relocation leak	UK, Afghanistan	Migrants, former interpreters, families	Resettlement applicant details and contact information	Secure casework for asylum/ relocation, least-privilege comms, emergency notification	Governments, NGOs, contractors; B2G/B2B SaaS	16
OPM	US	Employees, applicants, contractors, associates	SSNs, background files, fingerprints, sensitive history	Compartmentalised personnel systems, field-level encryption, hardware-key workflows	Government and govtech contractors; procurement + support	17

Case	Jurisdiction	Primary affected group	Data exposed or misused	Best-fit service or product	Likely payer and revenue model	Core sources
VTech	Hong Kong, US, Canada, global	Minors and parents	Child profiles, account data, photos, chats, audio	Children's privacy-by-design SDK, on-device storage, consent and deletion rails	Toymakers, edtech, OEMs; SDK licensing + compliance services	18
23andMe	US, UK, Canada, global	Consumers, protected ethnic groups, relatives	Ancestry, family tree, location, health and genetic data	Dynamic consent, mandatory MFA/ passkeys, relationship-graph minimisation	Genomics and digital-health firms; enterprise SaaS + governance tooling	19

The flow below captures the recurrent causal pattern across the case studies. The specific edges differ by sector, but the structure recurs with striking regularity across dating platforms, health systems, state casework, workforce-security systems, consumer genetics, and children's tech. 20



Case studies

Ashley Madison

Timeline and actors. In July 2015, "The Impact Team" hacked Ashley Madison's systems and threatened disclosure; on 18 and 20 August 2015, the attackers published data they claimed had been stolen from

roughly 36 million accounts. Canada's OPC and Australia's OAIC opened a joint investigation in August 2015, and the FTC later settled with Ruby Corp. and associated entities in December 2016. [21]

Data and harms. Official findings say the exposed material included profile information such as username, postcode, relationship status, gender, ethnicity, date of birth, and optional free-text fields like "My Intimate Desires". The official investigation also found that email addresses were not verified, meaning some non-users could be falsely associated with the service, and that "full delete" purchases did not fully delete all user data. Documented harms included extortion and scams, serious reputational harm to both users and wrongly associated non-users, and at least two unconfirmed suicides reported by Toronto police in connection with the leak. [22]

Legal outcome and lessons. The joint Canadian-Australian report found contraventions of PIPEDA and the Australian Privacy Act, after which ALM agreed to a Canadian compliance agreement and an Australian enforceable undertaking. The FTC's settlement required a comprehensive security programme and misrepresentation prohibitions. The main lesson is not simply "secure better"; it is **do not collect or retain intimate data you cannot defend**, and **deletion must mean deletion**. [23]

Mitigation, feasibility, and revenue angle. High-value mitigations include alias email or relay identities, optional contact channels, verified deletion with auditable erasure receipts, separation of billing identifiers from intimate profile content, and automated red-team testing of sign-up and deletion flows. Feasibility is high because these are mature design and infrastructure choices. The most obvious customers are dating platforms and adult-content services, with adjacent B2C revenue in privacy relays and post-breach identity-separation tools. [24]

Equifax

Timeline and actors. Attackers exploited a web-application vulnerability and maintained access between mid-May and July 2017; Equifax disclosed the breach publicly in September 2017. In 2019, the FTC, CFPB, and 50 U.S. states and territories reached a global settlement with Equifax. [25]

Data and harms. Official settlement materials state that hackers stole at least 147 million names and dates of birth, 145.5 million Social Security numbers, and 209,000 payment-card numbers and expiry dates. This is archetypal **identity-theft infrastructure** rather than mere embarrassment: the data are durable, difficult to rotate, and directly useful for fraud. The official consumer-relief programme continues to process claims for identity theft and fraud tied to the breach, which confirms that the injuries were not hypothetical. [26]

Legal outcome and lessons. The 2019 settlement totalled at least $575 million and potentially up to $700 million, including up to $425 million for consumer relief. The lesson is that static identifiers combined at scale create long-tail financial harm, meaning privacy rights here overlap with consumer-protection and anti-fraud rights. [27]

Mitigation, feasibility, and revenue angle. The strongest product response is not another generic alert service; it is a **consumer identity-defence control plane**: one-click credit freezes and thaws, doc-safe storage, passkey-first account hardening, breach-aware credential rotation, and guided fraud recovery. Feasibility is high. Natural buyers include banks, insurers, employers, unions, and payroll providers via B2B2C subscription bundles. [28]

Vastaamo

Timeline and actors. Vastaamo notified Finland's Data Protection Ombudsman of an attack in September 2020; in October 2020, patients were personally notified and then extorted; in December 2021 the Ombudsman imposed an administrative fine; in April 2024 a Finnish court sentenced Aleksanteri Kivimäki for the attack; and in February 2026 the appeal court increased the sentence to six years and eleven months. [29]

Data and harms. Public reporting and official findings describe the exposed material as highly sensitive psychotherapy records affecting more than 30,000 patients. The attacker first extorted the clinic and then attempted to extort individual patients, publishing data when payments were not made. Documented harms included blackmail, severe distress, and at least some reported suicides linked to the case; exact total causal attribution for all suicides is publicly contested, so precise numbers should be treated cautiously. [30]

Legal outcome and lessons. Finland's DPA fined Vastaamo for data-protection violations and had earlier ordered personal notification to affected customers. The former CEO was convicted in 2023 for data-protection failings, though reporting indicates that conviction was later overturned on appeal in December 2025. The broader lesson is that health privacy cannot be handled as ordinary CRM security: therapy notes require **content-level protections**, sharply limited retention, and tightly segregated access. [31]

Mitigation, feasibility, and revenue angle. Useful services include field-level or note-level encryption, split storage of identifiers and notes, zero-trust admin access, immutable audit logs, high-risk patient notification workflows, and trauma-informed breach support with counselling referrals. Feasibility is medium to high because the hardest part is operational redesign, not research novelty. Buyers are mental-health clinics, EHR vendors, telehealth providers, and cyber-insurers; revenue can come from enterprise software, managed security, and incident-response retainers. [32]

SpyFone

Timeline and actors. SpyFone operated from at least 2018; in August 2018 an unauthorised third party accessed its server; in 2021 the FTC finalised an order banning the company and its CEO from the surveillance business; and in December 2025 the FTC denied a petition to reopen or weaken that order. [33]

Data and harms. The FTC complaint states that SpyFone harvested emails, video chats, social-media activity, dating-app activity, photos, text messages, web histories, and GPS locations. The same complaint is unusually explicit about harm: stalkers and abusers can use such tools to monitor physical movements and online activities, causing mental and emotional abuse, financial and social harm, and physical harm, including death. This is one of the clearest official demonstrations that privacy loss can be a direct **personal-safety failure** rather than merely an informational one. [34]

Legal outcome and lessons. The FTC order banned SpyFone and its CEO from the surveillance business and required deletion of secretly harvested data. The continuing refusal to vacate that order in 2025 shows regulatory willingness to treat covert consumer surveillance as a structurally abusive business model. The lesson is that products marketed as "monitoring" tools can become abuse-enabling infrastructure unless they are designed with strong consent, visibility, and anti-misuse constraints. [35]

Mitigation, feasibility, and revenue angle. Strong mitigations include anti-stalkerware detection, OS-level integrity checks, carrier-supported safe-device replacement, survivor-safe account migration, and

integrated referral routes to domestic-abuse organisations. Feasibility is high. Market segments include mobile carriers, employers wanting device-integrity assurances, women's-safety NGOs, family-law practices, courts, and insurers. Revenue is plausible through carrier bundles, employer security services, and sponsored access for survivor-support networks. [36]

Grindr

Timeline and actors. The Norwegian Consumer Council filed complaints in 2020; Norway's DPA announced its intent to fine Grindr in January 2021 and imposed a NOK 65 million administrative fine in December 2021; the UK ICO issued a reprimand in July 2022; and public reporting shows UK compensation claims were filed in 2024. Public reporting in 2025 also indicates Grindr's appeal in Norway failed. [37]

Data and harms. The Norwegian decision found that Grindr disclosed user data to advertising partners without a valid legal basis and held that information showing a person is a Grindr user is data concerning sexual orientation within Article 9 GDPR. The decision also found that Grindr disclosed data to multiple advertising partners that could then propagate it within the adtech ecosystem. The public UK claim alleges users suffered distress, fear, embarrassment, and anxiety; official public records do not provide a settled tally of specific physical harms, so those remain unspecified in the available English-language record. [38]

Legal outcome and lessons. The legal outcomes include the Norwegian fine, the UK ICO reprimand, and ongoing compensation litigation. The core lesson is that **you do not need a classic hack for a privacy disaster**: placing sensitive-platform data into adtech pipelines can itself be a leak of socially consequential information. On LGBTQ+ platforms, contextual disclosure can create outing risk even when no field is literally labelled "sexual orientation". [39]

Mitigation, feasibility, and revenue angle. The best mitigations are product-level: no third-party adtech on sensitive platforms, no precise-distance defaults, private-by-default participation, on-device recommendation where possible, limited retention, screenshot and chat-safety controls, and premium privacy subscriptions instead of surveillance advertising. Feasibility is high because most levers are product and business-model choices. Revenue can come from premium subscriptions, B2B privacy SDKs for social apps, and enterprise trust-and-safety tooling. [40]

Pegasus against El Faro

Timeline and actors. Citizen Lab and partners documented Pegasus infections on devices belonging to Salvadoran journalists and civil-society members between July 2020 and November 2021. The findings were published in January 2022; the Inter-American Commission on Human Rights held a hearing in March 2022; El Faro members sued NSO Group in California in November 2022; and the Ninth Circuit revived the case in July 2025. [41]

Data and harms. Citizen Lab confirmed 35 cases and 37 infected devices, including at least 23 devices connected to El Faro. The lawsuit alleges at least 226 Pegasus infections affecting El Faro employees, through which iPhones were remotely accessed, communications and activities were monitored, and personal data were stolen. The newsroom has said it had to reconfigure its reporting practices as a result. This is a classic privacy-rights case because the harm is not only intrusion; it is the disablement of confidential reporting, source protection, and free expression. [42]

Legal outcome and lessons. As of July 2026, there is no final merits judgment in the El Faro case, but the Ninth Circuit's revival of the suit is itself consequential because it preserves a path to accountability

against a spyware vendor. The IACHR hearing also framed the abuse as a regional human-rights issue. The lesson is that high-risk users need privacy tools that assume **targeted compromise**, not only mass phishing. [43]

Mitigation, feasibility, and revenue angle. Relevant services include lockdown-by-default mobile configurations, compartmentalised newsroom devices, encrypted and ephemeral communications, incident-forensics retainers, legal escalation support, and security coaching for reporters and sources. Feasibility is medium: the threat model is hard, but the buyer need is real and urgent. Likely payers are newsrooms, NGOs, philanthropic security funds, and governments protecting diplomats or election monitors. [44]

UK Afghan relocation leak

Timeline and actors. In February 2022, a Ministry of Defence official exposed data relating to Afghan relocation applicants. The breach later became subject to a superinjunction; the government disclosed it publicly in July 2025 after High Court judgments lifted reporting restrictions; and the NAO reported on the resulting Afghanistan Response Route in September 2025. [45]

Data and harms. Government materials say the compromised dataset concerned 18,714 principal applicants to ARAP and the ex gratia scheme. Court materials and Reuters reporting make clear that the government itself argued public disclosure could expose people to extra-judicial killing or serious violence by the Taliban. Later survey reporting from refugee-support organisations and universities found widespread threats and severe mental-health effects among affected Afghans; those findings are not official government causation determinations, but they are serious documented evidence and should not be ignored. [46]

Legal outcome and lessons. The immediate legal response was secrecy and emergency relocation through a special route; later outcomes included High Court scrutiny, NAO review, a parliamentary inquiry, and active lawsuit preparation by affected individuals. The central lesson is that privacy failures in migration or relocation systems are often **life-safety failures with geopolitical consequences**. Here, confidentiality is not etiquette; it is part of protective infrastructure. [47]

Mitigation, feasibility, and revenue angle. Needed products include secure humanitarian case-management, role-based access, verified recipient controls, multilingual emergency notification workflows, automatic redaction, and secure evidence exchange with law firms and NGOs. Feasibility is medium to high; the technology exists, but procurement and operational discipline are the challenge. The primary market is B2G and NGO casework, with especially strong value in asylum, witness protection, and relocation programmes. [48]

OPM

Timeline and actors. By 2015, OPM disclosed linked breaches affecting personnel records and background-investigation files. Government materials ultimately concluded that sensitive information on 21.5 million individuals had been stolen. Congressional investigations followed, and a federal judge finalised a $63 million class settlement in 2022. [49]

Data and harms. Official notices state that the stolen information included Social Security numbers for 21.5 million individuals; background-investigation files contained information about mental health and financial history; and 5.6 million fingerprints were also stolen. National-security case materials described this information as extraordinarily useful for counter-intelligence, and reporting at the time

centered on blackmail, exploitation of foreign contacts, and exposure of covert personnel and their associates. Those harms are not reducible to ordinary consumer fraud. [50]

Legal outcome and lessons. The breach contributed to high-level resignations and later litigation. The 2022 settlement created a $63 million fund for demonstrable financial hardship, though reporting in 2025 suggested only a small fraction of that amount was ultimately paid out, which itself illustrates the mismatch between legal compensation and the real long-term exposure created by data theft. The lesson is that personnel and security-clearance systems should be designed for **segmentation, minimisation, and blast-radius control**. [51]

Mitigation, feasibility, and revenue angle. Valuable products include split-record architectures, field-level encryption, hardened administrator workflows, hardware-key-based access, protections for biometrics, and privacy-preserving background-check services that avoid centralising complete dossiers where possible. Feasibility is medium because incumbency and procurement complexity are high, but revenue potential is substantial in government and government-contractor markets. The same stack is relevant to whistleblowers and security-sensitive employees whose records could be weaponised. [52]

VTech

Timeline and actors. VTech's Learning Lodge and associated services were compromised in November 2015. Hong Kong's PCPD launched a compliance check immediately. In January 2018, the FTC announced a COPPA and security settlement, and Canada's Privacy Commissioner published investigation findings. [53]

Data and harms. Regulators found that millions of parents and children were affected. Reporting on the breach described exposure of customer details as well as children's photos, parent-child chat logs, and at least one audio recording. The concrete harm is partly current and partly long-tail: children cannot meaningfully consent, cannot easily rotate identity markers, and may carry exposure into later life. That is why children's privacy has special legal status rather than being treated as a subset of adult consumer choice. [54]

Legal outcome and lessons. The FTC settlement imposed a $650,000 penalty and remedial obligations under COPPA and the FTC Act, while Canada's OPC found inadequate safeguards; Hong Kong authorities also scrutinised the incident. The lesson is that **children's products must be private by architecture**, not by after-the-fact parental dashboards. [55]

Mitigation, feasibility, and revenue angle. Mitigations include on-device or edge storage, aggressive minimisation, short retention, no unnecessary media uploads, verifiable parental consent flows, strong deletion rights, and a reusable child-safety privacy SDK for connected toys and educational devices. Feasibility is high. Revenue fits OEM licensing, edtech compliance subscriptions, and certification or assessment services for school procurement. [56]

23andMe

Timeline and actors. A threat actor began credential-stuffing attacks in 2023; 23andMe disclosed the incident in October 2023. The UK ICO and Canada's OPC investigated jointly; the ICO issued a £2.31 million penalty in June 2025; the Canadian OPC found the safeguards contravened PIPEDA in June 2025; a U.S. class settlement received final approval in January 2026; and in July 2026 a bankruptcy judge approved a total $46.75 million payout for victims, while limiting California's ability to seek monetary relief from the successor entity. [57]

Data and harms. The ICO found that at least 155,592 UK users were affected and that exfiltrated data included ancestry reports, family-tree information, location, family names, profile pictures, birth years, health-related information, and some genetic data. The ICO also recorded evidence of "extreme anxiety" among affected users about personal, financial, and family safety, including concern that data had been targeted on racial and ethnic grounds. Reuters and the California AG both described the total global impact as nearly 7 million accounts. [58]

Legal outcome and lessons. This is already a multi-forum privacy case: UK penalty, Canadian findings, U.S. settlement, bankruptcy-court victim compensation, and state-attorney-general litigation. The key lesson is that genomic and relationship-graph data are **qualitatively different** from ordinary account data because they are hard or impossible to change and can expose information about relatives and protected groups, not just the account holder. [59]

Mitigation, feasibility, and revenue angle. Useful products include mandatory MFA or passkeys, dynamic consent and revocation tools, relationship-graph minimisation, granular sharing controls for relatives features, evidence-backed deletion, and governance tooling that treats genomic data as special-category data by default. Feasibility is medium to high. Natural buyers are genomics firms, digital-health platforms, biobanks, and research organisations; revenue comes from governance SaaS, independent assurance, and premium user control layers. [60]

Customer segments, go-to-market, and objections

A useful privacy business usually wins when it speaks to a **specific harm pathway** rather than to a generic moral preference. The personas below are derived from the case studies and from the regulatory expectation that organisations handling sensitive data use privacy by design, strong safeguards, and truthful interfaces. [61]

Segment and buyer persona	Pain proved by the cases	Product and service shape	Go-to-market message	Likely objection	Evidence-based rebuttal
Breach-experienced household. Buyer: consumer or employer benefits lead	Static identifiers and reused credentials create years of fraud and recovery burden	Identity-defence hub, breach-response concierge, passkey migration, freeze/thaw orchestration	"Turn privacy from paperwork into one-click containment."	"Consumers won't pay."	Consumers do pay when the pain is immediate; Equifax's relief programme and ongoing recovery claims show persistent demand, while OECD links trust in protections to digital participation. [62]

Segment and buyer persona	Pain proved by the cases	Product and service shape	Go-to-market message	Likely objection	Evidence-based rebuttal
Mental-health provider. Buyer: clinic CTO or privacy officer	Therapy records can be weaponised for blackmail and lasting trauma	Segmented EHR encryption, least-privilege admin, trauma-informed breach support	“Protect notes as if disclosure were itself a clinical emergency.”	“We already have cyber insurance.”	Insurance pays after loss; Vastaamo shows that once intimate notes escape, the harm is reputational and psychological as well as financial. [63]
Newsroom or NGO under pressure. Buyer: editor, operations director, security lead	Device compromise chills sources and alters reporting strategy	High-risk mobile security, secure source workflows, spyware forensics retainer	“Preserve source confidentiality under hostile-state conditions.”	“This is niche.”	It is niche by headcount but high-value by consequence. OHCHR and CISA both now recognise real surveillance harms and the need for stronger protections for highly targeted users. [64]
LGBTQ+ or dating platform. Buyer: chief product officer or trust-and-safety lead	Adtech and location defaults can out users and create discrimination risk	No-adtech sensitive stack, private-by-default UX, premium privacy controls	“Safety is the product, not an add-on.”	“Privacy features reduce monetisation.”	Regulators have already treated exploitative sharing as unlawful, and EDPB guidance explicitly frames privacy by design as a potential competitive advantage. [65]

Segment and buyer persona	Pain proved by the cases	Product and service shape	Go-to-market message	Likely objection	Evidence-based rebuttal
Domestic-abuse support ecosystem. Buyer: carrier, family-law network, NGO, insurer	Covert monitoring turns phones into abuse tools	Anti-stalkerware app, safe-device replacement, survivor workflow and referral tooling	“Stop the phone from being the abuser’s second body.”	“These tools could be used by criminals too.”	The FTC’s SpyFone complaint is clear that the dominant abuse pattern is stalking and domestic abuse, not legitimate parenting. CISA and OHCHR also explicitly support strong protective technologies for at-risk people. [66]
Government, relocation, or humanitarian casework. Buyer: programme director or contractor	Leaks can endanger lives and force costly emergency mitigation	Secure case-management, redaction, recipient verification, emergency messaging	“Confidentiality is resettlement infrastructure.”	“Government procurement is too slow.”	The UK Afghan case shows that the cost of failure can vastly exceed the cost of safer tooling; NAO documented a dedicated mitigation route and very large public expense. [67]

Segment and buyer persona	Pain proved by the cases	Product and service shape	Go-to-market message	Likely objection	Evidence-based rebuttal
Employer or govtech handling sensitive personnel records. Buyer: CISO or CHRO	Background and monitoring data can create blackmail, retaliation, and biometric exposure	Compartmentalised HR/clearance systems, hardware-key access, worker-safe monitoring policy	“Reduce dossier risk before the breach.”	“This is an edge case for security-cleared staff.”	OPM demonstrates that concentrated workforce data can become national-security-grade leverage. The same architectures also protect ordinary employees from overcollection. [68]
Children’s connected-product company. Buyer: founder, PM, or compliance lead	Minors’ photos, chats, and identifiers create high-sensitivity, long-lived exposure	Children’s privacy SDK, on-device media, consent and deletion rails, audit support	“Private by design is the easiest route to trust and procurement.”	“Parents, not kids, are the customer.”	The law disagrees: children receive special privacy protection, and VTech produced COPPA enforcement precisely because the product treated child data casually. [69]
Consumer genetics or digital health platform. Buyer: privacy officer or platform GM	Health, ancestry, and family-graph data create immutable disclosure risks	Dynamic consent, relationship-graph controls, passkeys, deletion and transfer governance	“When the data cannot be changed, the controls must be stronger.”	“Credential stuffing is just a user problem.”	The ICO rejected that framing in the 23andMe case and fined the company for inadequate organisational and technical controls. [70]

The most common objection to privacy businesses is the lazy claim that they “serve criminals”. That objection is weaker than it sounds. Official U.S. guidance now recommends end-to-end encrypted communications for highly targeted persons; governments have publicly acknowledged that strong encryption protects personal data, intellectual property, and journalists and vulnerable people; and OHCHR has explicitly linked encryption and anonymity to free opinion and expression. The evidence says privacy tools are mainstream defensive infrastructure, not inherently suspect goods. [71]

A second objection is that privacy is a compliance cost centre rather than a product differentiator. That is contradicted by both regulators and incidents. The EDPB explicitly encourages controllers, processors, and producers to use data protection by design and by default as a competitive advantage, while CISA’s secure-by-design work argues that manufacturers should carry more of the security burden so customers are less likely to be harmed. In markets touched by 23andMe, Grindr, VTech, and Ashley Madison, “trust” is no longer marketing decoration; it is a purchasing criterion with direct liability implications. [72]

A third objection is that users do not care enough about privacy to change behaviour. That is incomplete at best. People often do not buy privacy in the abstract because the risk is delayed and hard to price, but the economics literature identifies exactly those information asymmetries and market failures. OECD work also stresses that confidence in protections increases participation in the digital economy. The right commercial lesson is therefore not “users do not care”; it is “privacy products must translate diffuse risk into immediate user value”. [73]

Regulation, compliance, and ethical business practice

In the **EU**, the baseline is the GDPR plus sector-specific overlays. The GDPR treats health, genetic data, sexual orientation, and racial or ethnic origin as special categories needing extra protection, and personal-data breaches generally require notification to the supervisory authority unless the breach is unlikely to risk rights and freedoms; affected individuals must be informed when there is high risk. The ePrivacy regime still matters for communications confidentiality and tracking, and NIS2 adds broader cyber-governance expectations for entities in critical sectors. For privacy businesses, the practical implication is that **sensitive-data processing, incident response, and documentation discipline** are central readiness issues from day one. [74]

In the **UK**, the main framework is the UK GDPR together with the Data Protection Act 2018, supplemented by PECR for electronic communications and tracking contexts. The ICO’s current guidance emphasises the seven principles, especially integrity, confidentiality, and accountability, and separately stresses data protection by design and by default across the lifecycle of products and services. For a privacy company, the UK is therefore structurally favourable to products that can evidence privacy engineering, DPIAs, granular consent or lawful-basis management, and clear breach workflows. [75]

In the **United States**, privacy compliance is fragmented but still commercially demanding. There is no single federal omnibus law, but the FTC polices unfair or deceptive privacy and security practices; HIPAA and its Security and Breach Notification Rules cover health entities and business associates; the FTC’s Health Breach Notification Rule now clearly reaches many personal-health-record and health-app contexts; COPPA matters for children’s services; California gives residents rights over sensitive personal information; and all 50 states have breach-notification laws. The commercial lesson is that U.S. privacy products should be sold around **specific regulated workflows** rather than generic “GDPR-style” messaging. [76]

Among **other major markets**, Canada's PIPEDA requires reporting breaches that create a real risk of significant harm, plus individual notification and breach records. Singapore's PDPA requires notification to the PDPC no later than three calendar days after determining that a breach is notifiable. Brazil's ANPD rules require communication of reportable incidents within three working days. Australia's Notifiable Data Breaches scheme requires notice when a breach is likely to result in serious harm. For a privacy business with international ambitions, these regimes create strong demand for a single cross-market control layer handling data classification, incident triage, notification timing, and evidence retention. [77]

Ethically, privacy businesses should adopt a few operating rules if they want credibility rather than mere signalling. First, **collect less**: data minimisation and purpose limitation are not optional niceties. Second, **make privacy the default**, not a paid extra reserved for sophisticated users. Third, **avoid dark patterns** that trick users into giving up data. Fourth, **make deletion real and provable**. Fifth, **do not monetise sensitive data through opaque third-party sharing**, especially in health, children's, dating, or migration contexts. Sixth, build breach response that is **trauma-informed**, because the harms in cases like Vastaamo, SpyFone, Grindr, and the Afghan leak are not purely financial. These are not only moral preferences; they line up with current regulatory expectations in the EU, UK, and U.S. [78]

Finally, the most important practical distinction is between a privacy company that merely **helps users hide**, and one that **reduces the structural conditions under which their data becomes coercive power**. The second category is the stronger business and the stronger normative case. The research, the enforcement record, and the case studies all point the same way: privacy rights matter because information asymmetries become social power, and under common modern conditions that power can be abused at scale. [79]

---

[1] [5] [6] https://www.ohchr.org/en/UDHR/Documents/UDHR_Translations/eng.pdf
https://www.ohchr.org/en/UDHR/Documents/UDHR_Translations/eng.pdf

[2] [10] [20] [21] [23] https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-decisions/Investigation-inquiry-reports/ashley-madison-joint-investigation
https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-decisions/Investigation-inquiry-reports/ashley-madison-joint-investigation

[3] [12] [29] [30] [31] [32] [63] https://tietosuoja.fi/en/-/administrative-fine-imposed-on-psychotherapy-centre-vastaamo-for-data-protection-violations
https://tietosuoja.fi/en/-/administrative-fine-imposed-on-psychotherapy-centre-vastaamo-for-data-protection-violations

[4] [61] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-by-default/
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-by-default/

[7] https://www.oecd.org/en/topics/policy-issues/privacy-and-data-protection.html
https://www.oecd.org/en/topics/policy-issues/privacy-and-data-protection.html

[8] [64] https://www.ohchr.org/en/documents/studies-and-research/pushed-shadows-evidencing-digital-surveillance-chilling-effects-and
https://www.ohchr.org/en/documents/studies-and-research/pushed-shadows-evidencing-digital-surveillance-chilling-effects-and

[9] https://nvlpubs.nist.gov/nistpubs/ir/2017/nist.ir.8062.pdf
https://nvlpubs.nist.gov/nistpubs/ir/2017/nist.ir.8062.pdf

11 26 https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach
https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

13 33 34 66 https://www.ftc.gov/system/files/documents/cases/1923003c4756spyfonecomplaint_0.pdf
https://www.ftc.gov/system/files/documents/cases/1923003c4756spyfonecomplaint_0.pdf

14 38 39 40 65 https://www.datatilsynet.no/contentassets/8ad827efefcb489ab1c7ba129609edb5/administrative-fine---grindr-llc.pdf
https://www.datatilsynet.no/contentassets/8ad827efefcb489ab1c7ba129609edb5/administrative-fine---grindr-llc.pdf

15 41 42 https://citizenlab.ca/research/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/
https://citizenlab.ca/research/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/

16 47 https://www.judiciary.uk/wp-content/uploads/2025/07/MOD-Judgment-No-4-final.pdf
https://www.judiciary.uk/wp-content/uploads/2025/07/MOD-Judgment-No-4-final.pdf

17 49 50 68 https://www.doi.gov/cybersecurity-update
https://www.doi.gov/cybersecurity-update

18 55 https://www.ftc.gov/news-events/news/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated-childrens-privacy-law-ftc-act
https://www.ftc.gov/news-events/news/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated-childrens-privacy-law-ftc-act

19 57 59 https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/
https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/

22 24 https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/
https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/

25 https://investor.equifax.com/news-events/press-releases/detail/240/equifax-announces-cybersecurity-incident-involving-consumer
https://investor.equifax.com/news-events/press-releases/detail/240/equifax-announces-cybersecurity-incident-involving-consumer

27 https://www.consumerfinance.gov/enforcement/actions/equifax-inc/
https://www.consumerfinance.gov/enforcement/actions/equifax-inc/

28 62 https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement
https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

35 https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3003-support-king-llc-spyfonecom-matter
https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3003-support-king-llc-spyfonecom-matter

36 https://refuge.org.uk/i-need-help-now/how-we-can-help-you/secure-your-tech/
https://refuge.org.uk/i-need-help-now/how-we-can-help-you/secure-your-tech/

37 https://www.reuters.com/technology/grindr-faces-117-mln-fine-norway-breach-data-privacy-2021-01-26/
https://www.reuters.com/technology/grindr-faces-117-mln-fine-norway-breach-data-privacy-2021-01-26/

43 https://knightcolumbia.org/content/appeals-court-revives-journalists-case-against-spyware-manufacturer-nso-group
https://knightcolumbia.org/content/appeals-court-revives-journalists-case-against-spyware-manufacturer-nso-group

44 https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf
https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf

45 https://www.gov.uk/government/speeches/oral-statement-on-afghan-data-breach
https://www.gov.uk/government/speeches/oral-statement-on-afghan-data-breach

46 https://refugeelegalsupport.org/legal-information-pages/data-breach-factsheet
https://refugeelegalsupport.org/legal-information-pages/data-breach-factsheet

48 67 https://www.nao.org.uk/reports/the-afghanistan-response-route/
https://www.nao.org.uk/reports/the-afghanistan-response-route/

51 https://federalnewsnetwork.com/workforce/2022/10/federal-judge-finalizes-63m-settlement-for-opm-data-breach-victims/
https://federalnewsnetwork.com/workforce/2022/10/federal-judge-finalizes-63m-settlement-for-opm-data-breach-victims/

52 71 https://www.cisa.gov/resources-tools/resources/mobile-communications-best-practice-guidance
https://www.cisa.gov/resources-tools/resources/mobile-communications-best-practice-guidance

53 https://www.pcpd.org.hk/english/news_events/media_statements/press_20151201c.html
https://www.pcpd.org.hk/english/news_events/media_statements/press_20151201c.html

54 https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180108/
https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180108/

56 https://www.edpb.europa.eu/documents/guideline/guidelines-42019-on-article-25-data-protection-by-design-and-by-default_en
https://www.edpb.europa.eu/documents/guideline/guidelines-42019-on-article-25-data-protection-by-design-and-by-default_en

58 60 70 https://ico.org.uk/media2/kclbljpo/23andme-penalty-notice.pdf
https://ico.org.uk/media2/kclbljpo/23andme-penalty-notice.pdf

69 https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child
https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

72 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

73 79 https://www.aeaweb.org/articles?id=10.1257%2Fjel.54.2.442
https://www.aeaweb.org/articles?id=10.1257%2Fjel.54.2.442

74 https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-basics_en
https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-basics_en

75 https://www.gov.uk/data-protection
https://www.gov.uk/data-protection

76 https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

77 https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-3.html
https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-3.html

78 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/