

Privacy, Security, and the Ethics of Resisting Lawful Extraction

The ethical baseline

Privacy and security are not merely tactical conveniences for wrongdoers. In the philosophical literature, privacy is tied to **autonomy, intimacy, control over access to oneself, and the conditions for a free and self-authored life**; in medical ethics it also protects bodily integrity, confidentiality, associational privacy, and decisional freedom. Human-rights doctrine treats interference with privacy as something that must satisfy **separate** tests of legality, necessity, and proportionality, which means even an authorised intrusion is not automatically a justified one. ¹

That distinction matters because “lawful” is a status inside a legal system, whereas “ethical” is a judgment about what people and institutions ought to do. A domestic rule can be procedurally valid and still be abusive, overbroad, discriminatory, or indifferent to human dignity. European and UN materials make this explicit by requiring not only a legal basis, but also **strict necessity, proportionate design, clear limits, and safeguards against abuse** whenever privacy is restricted. ²

From that starting point, the ethical case for supporting strong privacy and security even against some “lawful” extractions is straightforward: these protections defend people not only against criminals, but also against **state error, state overreach, politically opportunistic enforcement, compelled third-party disclosure, reputational ruin, and irreversible data exposure**. The argument is not that every investigation is wrong. It is that **privacy is a presumptive good**, and the burden of justification lies with the intruder, not with the person who wishes to keep their life opaque. ³

Why legality does not settle morality

The clearest reason law and ethics come apart is that unjust laws exist, and sometimes remain in force for long periods. Contemporary human-rights reporting still documents **more than 60 jurisdictions** that criminalise consensual same-sex sexual conduct. That is enough, by itself, to show that “the state says this is illegal” cannot serve as a moral trump card. If the law can still punish identity, intimacy, or association, then resisting legal intrusion can sometimes be an act of self-respect rather than evasion. ⁴

The mainstream philosophical tradition on civil disobedience does not treat all law-breaking as nihilistic or antisocial. It treats some law-breaking as **conscientious, public-minded resistance** aimed at reforming unjust laws or policies, often while accepting legal risk. Martin Luther King Jr.’s *Letter from Birmingham Jail* is the canonical political example: he distinguished just from unjust laws and argued that disobedience to the latter can express, rather than negate, fidelity to deeper legal and moral principles. ⁵

That matters for privacy because some investigations are not ethically neutral fact-finding exercises. They can be mechanisms for enforcing bad laws, selectively punishing stigmatised groups, or suppressing disfavoured dissent. When the underlying norm is unjust, or when enforcement is discriminatory, **shielding oneself from state visibility** can be ethically justified in the same way that

other forms of civil disobedience can be justified. That is especially true where exposure would not simply lead to adjudication of a discrete offence, but to lifelong stigma, extortion, family danger, or political retaliation. ⁶

Why digital extraction is unusually invasive

Modern device and account extraction is not morally equivalent to checking a single paper document or searching a single room. Cellebrite markets tools for **full file system and physical extractions**, and its “Premium” offering advertises the ability to **unlock, decrypt, and extract** evidence from locked iOS and Android devices. Apple says account requests may seek not only subscriber details but also **photos, email, device backups, contacts, and calendars**. Google states that warrants can compel disclosure of content from **Gmail, Drive, and Photos**, and that it may be legally forbidden to notify the user while a gag period is in force. ⁷

Ethically, that breadth matters because the target is rarely just the suspect’s own information. Phones and cloud accounts are dense archives of **third-party conversations, intimate images, health information, location histories, political affiliations, professional confidences, and social graphs**. Swedish data-protection guidance classifies health data, sexual life, sexual orientation, political opinions, religion, genetics, and biometrics as specially sensitive categories of data. A forensic extraction can therefore expose not just one person’s possible wrongdoing, but the private worlds of partners, children, patients, clients, colleagues, and sources. ⁸

For precisely that reason, European privacy law does not accept “lawful access exists” as a sufficient ethical or legal answer. The CJEU has held that general and indiscriminate transmission of communications traffic and location data to security agencies **exceeds what is strictly necessary**, and the European Court of Human Rights held in *Big Brother Watch* that aspects of the UK’s bulk interception regime and its regime for obtaining communications data from service providers violated Articles 8 and 10. The governing principle is not “if authorised, then fine.” It is **strict necessity plus adequate safeguards**. ⁹

The Apple–UK dispute gives a concrete example of why resistance can itself be ethical. In 2025 Apple challenged the Home Secretary’s use of Technical Capability Notices before the Investigatory Powers Tribunal, and Apple later withdrew Advanced Data Protection for new UK users rather than build a “backdoor or master key.” Human Rights Watch and Amnesty argued that the reported order threatened privacy rights globally, because the demanded access would have affected encrypted cloud data far beyond a single suspect or a single case. On this model, resisting a lawful demand is not contempt for justice; it is refusal to **weaken the security baseline for everyone**. ¹⁰

Why formal due process is not enough

Criminal procedure itself recognises that innocence is not protected simply by letting investigators ask anything and seize everything. EU law states that the **right to remain silent** and the **right not to incriminate oneself** are important aspects of the presumption of innocence, and the European Court of Human Rights has said that the prosecution should prove its case **without resort to evidence obtained through coercion or oppression in defiance of the accused’s will**. The logic behind that rule is structural: even innocent people can be trapped, misread, worn down, or turned into evidentiary raw material for the state. ¹¹

That procedural caution is justified by the frequency of miscarriage. The European Registry of Exonerations currently records **144 exonerations across 20 countries** and **927 years incarcerated in**

total. In the United States, the National Institute of Justice notes that the National Registry of Exonerations has recorded **over 3,000 wrongful convictions**, while the Innocence Project reports that misapplied forensic science contributed to **more than half** of its cases and nearly a quarter of wrongful-conviction cases since 1989. False confessions remain an established cause of wrongful conviction as well. ¹²

Digital evidence does not dissolve these problems; in some respects it intensifies them. NIST's review of digital investigation techniques says the methods are reliable **when used appropriately**, but also warns that not all evidence will be discovered, deleted-file recovery can include extraneous material, and the meaning of digital artefacts can change as software evolves. The UK Forensic Science Regulator similarly warns that digital forensic work must address uncertainty, and notes that a timestamp can be highly precise **without thereby being accurate**. The same regulator's 2026 guidance also emphasises that interpretation is not automatic: forensic findings may be merely investigative, evaluative, analytical, categorical, or purely factual, and those forms should not be confused. ¹³

That is the core epistemic problem behind the user's intuition that "rättssäkerhet" can become theatre. **A legally staged process can still overread ambiguous artefacts.** Geofence warrants are a current illustration: civil-liberties groups and courts have criticised them precisely because they sweep in large numbers of innocent bystanders and let police decide later whom to focus on. ACLU litigation in 2026 described geofence warrants as compelling Google to turn over location data from every device probably present within an area and time window, after which investigators select who to scrutinise further. Nearby technologies show the same danger: the ACLU's 2026 case *Dillon v. City of Jacksonville Beach* alleges a wrongful arrest after police relied on a false facial-recognition result and then let that result taint later investigative steps. ¹⁴

Once that risk is taken seriously, resistance to extraction no longer looks like a purely guilt-signalling act. It can instead be seen as a refusal to let the state construct a narrative from **high-volume, high-context, error-prone evidence** under institutional pressures that often reward closure rather than epistemic humility. That is not a proof that every extraction is wrong; it is a reason not to assume that court supervision or formal legality has solved the ethical problem. ¹⁵

Why disclosure and retention can cause irreversible harm

Even when the state obtains information lawfully, the harmful act is not over at the moment of collection. The data now exists inside systems with their own publicity rules, sharing rules, breach risks, and reputational dynamics. Sweden is an especially vivid example. The National Board of Forensic Medicine states that forensic psychiatric reports are based not only on psychiatric examination, but also on records and journals obtained from healthcare contacts, the Prison and Probation Service, the Migration Agency, and social services. At the same time, Swedish courts explain that **most documents in court proceedings are public documents**, that materials filed in a case generally become public records, and that court hearings are ordinarily public. ¹⁶

The exposure risk becomes stronger when courts themselves reproduce sensitive information. In a 2025 decision, the Swedish Supreme Court stated that criminal judgments are public as a starting point and that, **if information is included in a judgment, any secrecy attached to that information ceases unless the court orders continued secrecy**. Swedish privacy guidance classifies health data and sexual orientation as sensitive personal data. Put together, those rules mean that information lawfully pulled into a criminal process can move from confidential settings into a public judgment unless specific protective decisions are made. Ethically, that is a powerful reason to support privacy and

security against extraction in the first place: some harms cannot be undone once the information has circulated. ¹⁷

Nor is the danger limited to official publication. Data stockpiles leak. Sweden's privacy regulator fined Sportadmin in 2026 after a 2025 cyberattack exposed the data of **more than 2.1 million individuals**, mainly children and young people, with the data later published on the darknet. The lesson is general: data that has been lawfully collected and centrally stored remains vulnerable to accidental disclosure, negligent security, hostile insiders, and outright compromise. From an ethical perspective, **data minimisation is not anti-investigative dogma; it is harm prevention.** ¹⁸

This is also why provider compulsion is morally weighty even when issued under proper process. Google states that it normally notifies users before disclosure, but that it will not do so when legally prohibited, including during court-ordered or statutory gag periods. A person can therefore be subjected to covert extraction from their account without a chance to contest scope, necessity, or downstream use at the moment it matters most. Ethical support for privacy and encryption is partly support for **keeping less extractable material available in the first place.** ¹⁹

Why journalists, activists, and dissidents have special claims

The case for resisting surveillance becomes stronger, not weaker, when the target is engaged in democratic accountability. UN and human-rights materials have repeatedly said that **encryption and anonymity are essential** for the exercise of freedom of expression in the digital age, and Amnesty has stressed that encryption is particularly critical for **human-rights defenders, activists, and journalists.** In 2026 the UN Special Rapporteur on freedom of assembly and association warned that digital surveillance creates durable chilling effects on association and protest. The point is not abstract: if people reasonably fear that source networks, organising chats, or attendance patterns will be extracted, many will simply stop speaking or assembling. ²⁰

Real-world cases show that this is not paranoia. Citizen Lab and partners confirmed **35 Pegasus infections** among journalists and civil-society figures in El Salvador. In 2024 Citizen Lab also found Pegasus targeting of **Russian and Belarusian-speaking opposition activists and independent journalists in Europe.** In 2026 Citizen Lab reported that a former Member of the European Parliament serving on the committee investigating spyware abuses had himself been hacked with Pegasus. These are precisely the sorts of cases in which the official line is often "lawful national security" while the ethical reality is intimidation, source compromise, and democratic degradation. ²¹

Serbia supplies an even closer example to the user's concern about Cellebrite. Amnesty reported in late 2024 that Serbian authorities used **Cellebrite forensic extraction tools** together with bespoke spyware to target journalists and activists, including infections during detention or police interviews. In 2025 Amnesty documented a further case in which a **Cellebrite zero-day exploit** was used against a student activist's Android phone, and noted that Cellebrite had suspended relevant customers in Serbia after reviewing the earlier allegations. When tools built for "lawful extraction" become part of a repression pipeline, resistance to extraction is no longer just self-protection; it is defence of civic space. ²²

Journalists also have a distinct source-protection interest recognised in European law. The European Court of Human Rights has repeatedly stressed the importance of protecting journalistic sources, and a UK tribunal ruled in 2024 that Northern Ireland police had unlawfully surveilled journalists Trevor Birney and Barry McCaffrey without properly considering the overriding public interest in protecting journalistic sources. If powerful actors can compel device access or communications data from reporters with ease, source protection becomes formal rhetoric rather than practical reality. ²³

When resistance is ethically justified

A reasonable synthesis of the sources is that resistance to an investigation can be ethically justified when several features converge. The case is strongest where the **underlying law is itself unjust** or discriminatorily enforced; where the measure is **overbroad** relative to the allegation; where it predictably captures **third-party confidences**; where the institution demanding access has poor safeguards, poor reliability, or a history of abuse; where the target has a recognised democratic function such as journalism, defence, or human-rights advocacy; and where disclosure would impose **irreversible harms** that far exceed the legitimate needs of the inquiry. Those conditions track the civil-disobedience tradition, the presumption of innocence, the privilege against self-incrimination, and the privacy law requirements of necessity and proportionality. ²⁴

That does **not** amount to a blanket ethical licence to obstruct justice. The same source base points in the other direction where authorities are pursuing a genuinely grave and imminent harm, the access sought is narrowly tailored, independently reviewed, and demonstrably the least intrusive workable means, and the main effect of resistance would be to preserve the capacity to continue seriously harming others. Human-rights law does not make privacy absolute; it makes intrusion a matter of heavy justification. The ethical position is therefore not “always comply” or “always resist,” but **start from privacy, then justify exceptions under necessity, proportionality, and institutional trustworthiness.** ²⁵

The most defensible bottom line is this: **supporting privacy and security even against some lawful extractions is not anti-law by definition.** It is often support for autonomy, fair process, democratic accountability, third-party protection, and damage control in systems that are legal yet fallible, and sometimes legal yet unjust. In that framework, there really are cases in which breaking the law, refusing visibility, or resisting an investigation is ethically justified—not because truth or justice do not matter, but because truth and justice are not well served by treating state access as morally self-validating. ²⁶

¹ ³ ²⁶ Privacy - Stanford Encyclopedia of Philosophy

https://plato.stanford.edu/entries/privacy/?utm_source=chatgpt.com

² ⁹ Mass surveillance

<https://ks.echr.coe.int/documents/d/echr-ks/mass-surveillance>

⁴ Breaking the Silence: Criminalisation of Lesbians and ...

https://www.humandignitytrust.org/resources/breaking-the-silence-criminalisation-of-lesbians-and-bisexual-women-and-its-impacts-summary/?utm_source=chatgpt.com

⁵ ²⁴ Civil Disobedience - Stanford Encyclopedia of Philosophy

https://plato.stanford.edu/entries/civil-disobedience/?utm_source=chatgpt.com

⁶ Map of Jurisdictions that Criminalise LGBT People

https://www.humandignitytrust.org/lgbt-the-law/map-of-criminalisation/?utm_source=chatgpt.com

⁷ Cellebrite UFED | Mobile Forensic Data Extraction Tool

https://cellebrite.com/en/products/ufed/?utm_source=chatgpt.com

⁸ Känsliga personuppgifter | IMY

<https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter/>

¹⁰ Apple Inc v Secretary of State for the Home Department - The Investigatory Powers Tribunal

<https://investigatorypowerstribunal.org.uk/judgement/apple-inc-v-secretary-of-state-for-the-home-department/>

11 Directive - 2016/343 - EN - EUR-Lex

<https://eur-lex.europa.eu/eli/dir/2016/343/oj/eng>

12 Home

<https://www.registryofexonerations.eu/>

13 15 Digital Investigation Techniques: A NIST Scientific Foundation Review | NIST

<https://www.nist.gov/publications/digital-investigation-techniques-nist-scientific-foundation-review>

14 Nguyen v. State | American Civil Liberties ...

https://www.aclu.org/cases/nguyen-v-state?utm_source=chatgpt.com

16 Rättspsykiatrisk undersökning - Rättsmedicinalverket

<https://www.rmvm.se/verksamheter/rattspsykiatri/rattspsykiatrisk-undersokning/>

17 domstol.se

<https://www.domstol.se/globalassets/filer/domstol/hogstodomstolen/avgoranden/2025/a-3169-24.pdf>

18 Administrative fine against Sportadmin

https://www.imy.se/en/news/administrative-fine-against-sportadmin/?utm_source=chatgpt.com

19 How Google handles government requests for user information – Privacy & Terms – Google

<https://policies.google.com/terms/information-requests?hl=en-US>

20 A/HRC/29/32: Report on encryption, anonymity, and the ...

https://www.ohchr.org/en/documents/thematic-reports/ahrc2932-report-encryption-anonymity-and-human-rights-framework?utm_source=chatgpt.com

21 Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware - The Citizen Lab

<https://citizenlab.ca/research/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/>

22 Serbian authorities using spyware to hack activists and journalists

<https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists/>

23 Protection of journalistic sources | ECHR

https://www.echr.coe.int/documents/d/echr/fs_journalistic_sources_eng?utm_source=chatgpt.com

25 International standards

https://www.ohchr.org/en/privacy-in-the-digital-age/international-standards?utm_source=chatgpt.com