

Palm Vein Reconstruction From Electromagnetic Side-Channel Emissions: Public Perceptions of Privacy Risks

Ziwen Lu

ziwenlu@snina.cn

Wenzhou Medical University

P.F. Hu

Brown University

X. Gao

Shandong University

Research Article

Keywords: biometric privacy, palm vein, public perceptions, privacy risk, institutional trust, data protection

Posted Date: August 24th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10771346/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Additional Declarations: The authors declare no competing interests.

Abstract

Biometric authentication is often presented as a more secure alternative to passwords because bodily characteristics are difficult to share, forget, or casually reproduce. That advantage also makes compromise unusually consequential: biometric attributes cannot be reset in the same way as a password. Recent technical work has shown that palm-recognition systems can present confidentiality risks when unintended electromagnetic emissions are treated as an attack surface. This paper does not reproduce, test, or describe such an attack. Instead, it asks a psychosocial question: what pre-existing public attitudes toward online recording, data protection, institutional trust, and identity-protection practices provide the social context in which people may interpret an emergent biometric privacy risk? We conduct a transparent secondary analysis of public aggregate tables from Special Eurobarometer 359, fielded in 2010 across the EU27 (N = 26,574). The survey does not measure palm-vein systems or electromagnetic side channels directly. It is used as a historically situated baseline for general digital-identity and privacy-risk perceptions, not as evidence of attitudes to a specific device vulnerability. Forty percent of respondents were concerned about online behaviour being recorded, while only 22% trusted internet companies to protect personal information. Among people who had disclosed information on social or sharing sites, 20% reported no control at all over that information; among social or sharing-site users, 51% had tried to change default privacy settings. Country-level concern and trust showed no meaningful linear association. The findings indicate that a technical disclosure involving biometric leakage would enter a public environment marked by substantial concern, weak trust in internet intermediaries, and incomplete perceptions of control. The paper develops implications for risk communication, governance, and future scenario-based research. Its principal contribution is to connect an engineering-defined biometric vulnerability with the social conditions that shape whether privacy protections are understandable, credible, and actionable.

1. Introduction

Biometric systems convert characteristics of the body or behaviour into credentials. Their appeal is intuitive. A person does not need to remember a password, carry a token, or perform a complex account-recovery procedure. The same property that supports convenience, however, complicates privacy. A stolen password can be changed; a compromised bodily characteristic cannot be replaced in an equivalent way. This asymmetry has long made biometric technologies a special case for information-security and privacy scholarship [3] [4] [5]. It also makes it inadequate to assess biometric risk only through the engineering performance of a sensor or matching algorithm. The social meaning of a leak matters: people need to understand what has been exposed, who may be responsible, what control they retain, and what protective action is possible.

The paper title is deliberately close to an emerging technical research problem: **Palm Vein Reconstruction From Electromagnetic Side-Channel Emissions**. Recent technical publications demonstrate that unintended electromagnetic emanations from palm-recognition equipment can challenge assumptions of biometric confidentiality [1] [2]. This article does not operationalise, repeat,

validate, or extend those technical findings. It provides no instructions about signal collection, device inspection, biometric reconstruction, authentication bypass, or attack optimisation. The focus is the public-facing side of the problem: the privacy concerns, control perceptions, trust judgments, and self-protection practices that are likely to condition how people react when a biometric data risk is disclosed.

That shift is relevant to cyberpsychology. Security incidents are not only events in systems. They are also events in interpretation. A vulnerability notice can raise anxiety, alter willingness to share information, decrease trust in a service provider, or prompt protective behaviour. Conversely, vague notice language, technical opacity, and weak institutional credibility can generate resignation rather than meaningful action. Research on information privacy shows that people's decisions are shaped by uncertainty, context, cognitive constraints, social expectations, and unequal institutional power [9] [10]. The same factors are likely to matter when a risk involves biometric data, because the object of concern is not an abstract account identifier but information tied to the body and identity.

There is an important empirical difficulty. Large, public, cross-national surveys rarely ask respondents about palm-vein recognition or electromagnetic side-channel emissions. It would be methodologically unsound to pretend otherwise. This study therefore treats the technology-specific phrase in the title as an **illustrative risk context**, while its empirical analysis is restricted to measures that the public dataset actually contains: concern about online behaviour being recorded; control over disclosed information; default privacy-setting changes; trust in institutions that hold personal information; experiences and awareness of identity-theft and data-loss issues; and preferences for special protection of sensitive genetic information. The study asks what these observable attitudes reveal about the broader social climate into which a biometric leakage disclosure would arrive.

Special Eurobarometer 359, *Attitudes on Data Protection and Electronic Identity in the European Union*, offers a useful and transparent baseline. The European Commission fielded the survey in November–December 2010, and the official public tables report results for 26,574 respondents in the EU27 [16]. The dataset predates today's broad deployment of palm-based biometric systems and cannot be read as a current prevalence estimate. Its value is different. It captures public beliefs about electronic identity, personal-data protection, online recording, social-web disclosure, and institutional responsibility before these questions became further embedded in contemporary platform and AI policy. These measures make it possible to distinguish public concern from public control, and technical risk from trust in the institutions expected to manage that risk.

The analysis addresses four research questions. **RQ1** asks how prevalent concern about online behaviour being recorded was in the EU27 baseline. **RQ2** asks how concern differed across demographic and behavioural groups and how it related to perceived control over disclosed social-web information. **RQ3** asks whether trust in institutions, particularly internet companies, was commensurate with the sensitivity of the information at issue. **RQ4** asks what public identity-protection behaviours and cross-country patterns suggest about the limits of individual responsibility for a prospective biometric privacy

threat. These questions do not test whether a named side-channel attack is feasible. They test the social conditions under which its communication and governance would be received.

2. Biometric Privacy as a Psychosocial Problem

2.1 Why biometric risks are socially distinctive

Biometric recognition commonly relies on physical or behavioural traits to establish identity. Foundational research has emphasised both its convenience and its security advantages, but it has also highlighted the need to protect stored templates, acquisition devices, and system interfaces [3] [4]. The privacy issue is not simply that a record exists. A biometric representation may be persistent, difficult to revoke, usable across contexts, and capable of linking an individual to services or spaces. Campisi [5] argues that security and privacy must be treated as joint requirements rather than as a trade-off imposed after deployment.

Public attitudes to biometrics do not reduce neatly to a choice between privacy and security. Norval and Prasopoulou's qualitative study identified multiple public positions that complicate the conventional claim that citizens simply exchange privacy for protection [6]. Kugler's experimental work similarly found that members of the public can view biometric harms as serious in consumer contexts and may be willing to sacrifice benefits to avoid them [7]. Recent research continues to show that risk perception, trust, and governance expectations shape intentions toward biometric information use [8]. These findings matter because a technically sophisticated safeguard does not automatically create legitimacy. People judge the collection and processing of bodily data against expectations about control, fairness, purpose limitation, and institutional accountability.

Palm-vein recognition adds an additional layer to this discussion. The modality is often described as concealed or difficult to copy because it uses internal vascular patterns. A public claim that such data could be exposed through unintentional emissions may therefore challenge a perception of inherent safety. In this paper, the relevant psychosocial outcome is not fear of a particular scientific mechanism. It is the possibility of an expectation violation: a credential presumed to be securely bound to the body becomes, in the public imagination, another form of data that may be collected, inferred, retained, or misused. The technical literature motivates the risk context [1] [2], but public responses depend on privacy beliefs that exist before any device-specific explanation is offered.

2.2 Privacy concern, uncertainty, and contextual integrity

Privacy scholarship has repeatedly warned against treating concern as a simple personality trait. Acquisti, Brandimarte, and Loewenstein [9] describe privacy behaviour as shaped by uncertainty about consequences, context-dependent preferences, and powerful design and institutional influences. Smith, Dinev, and Xu [10] organise an extensive literature around antecedents, privacy concerns, and outcomes, noting that individual concern is embedded in organisational and societal contexts. Their framework is

especially useful here because a biometric side-channel disclosure can be interpreted as a new antecedent: it changes beliefs about the likelihood and consequences of information exposure.

The perceived-risk literature also identifies privacy concern as a driver of transaction and disclosure decisions. Dinev and Hart [12] show that internet privacy concerns, social awareness, and internet literacy are relevant to willingness to transact online. Malhotra, Kim, and Agarwal [11] conceptualise internet users' information privacy concerns through collection, control, and awareness. These dimensions map closely onto a biometric leak scenario. People may ask whether a biometric trait was captured beyond what was necessary, whether they can influence the processing of that information, and whether a provider had informed them about the relevant risk.

Context is central. Nissenbaum's theory of contextual integrity argues that privacy is not merely secrecy; it is the appropriateness of information flows relative to social norms, actors, and transmission principles [13]. Solove's taxonomy likewise shows that privacy harms include collection, processing, dissemination, and invasion rather than a single act of disclosure [14]. A palm-vein system used for building access, payment, health service entry, or workplace timekeeping may evoke different expectations even when it uses the same underlying modality. This is why the current study does not infer a single universal "biometric concern" score from generic privacy data. It instead examines several dimensions—recording concern, control, trust, and protection behaviour—that together describe the interpretive environment.

2.3 The privacy paradox, control, and protective action

Concern does not always become protective behaviour. Taddicken [15] found that privacy concerns alone had limited direct influence on self-disclosure, while social relevance, application use, and individual conditions mattered. This pattern, often called the privacy paradox, should not be read as proof that users do not care. It may reflect constrained choice, weak usability, low perceived efficacy, or a mismatch between the action a person can take and the risk they face. Those issues become acute for biometric systems. A user can delete cookies or change a profile setting, but cannot independently inspect sensor hardware or revoke a vascular pattern that has already been captured.

Perceived control is therefore analytically important. If people feel they have only partial or no control over information disclosed online, a message that asks them to "manage their privacy" may be less credible than an institutional remedy. The same is true of trust. Confidence in a service provider determines whether a statement about mitigation will be accepted as assurance or dismissed as reputation management. For public-facing biometric systems, the appropriate response to a technical vulnerability should thus involve meaningful provider obligations, understandable disclosure, and accessible redress—not only advice to the individual user.

2.4 Contribution

The paper makes three contributions. First, it reframes an engineering-defined biometric leakage risk as a question of public privacy perception without revealing operational details. Second, it uses a large,

official, cross-national public dataset to distinguish concern, control, trust, and self-protection rather than relying on a single generic measure. Third, it makes the proxy status of the evidence explicit. The survey measures broad electronic-identity and online privacy attitudes, not respondents' awareness of palm-vein technologies or side-channel emissions. This transparency is crucial for a responsible interdisciplinary account of emerging technology risks.

3. Method

3.1 Design and data source

This study is a descriptive secondary analysis of the public statistical tables from Special Eurobarometer 359, *Attitudes on Data Protection and Electronic Identity in the European Union* [16]. The European Commission's public data portal identifies the resource as a survey of citizens' behaviours and attitudes concerning identity management, data protection, and privacy. The official table files are publicly accessible and include EU-level results, country comparisons, and social-demographic breakouts. The fieldwork occurred during November and December 2010. The EU27 total in the relevant tables is 26,574 respondents.

The study uses published aggregate tables rather than confidential individual records. This choice has two advantages. It makes every reported descriptive statistic traceable to the public source, and it avoids overstating precision by fitting individual-level models to data that are not publicly distributed in the analysis package used here. The limitation is equally clear: aggregates do not permit causal inference, multivariable adjustment, individual-level interactions, or a direct test of whether a person who is concerned also changes settings. The analysis is intentionally descriptive and contextual.

The source is appropriate for an electronic-identity baseline because it includes questions about online recording, social-network disclosure, privacy settings, institutional trust, identity protection, data loss, identity theft, and sensitive data protection. Eurobarometer 83.1, fielded in 2015, contains related data-protection and internet measures and confirms the wider availability of this family of public survey resources [17]. It is not pooled with the 2010 tables here, because question wording, sample composition, and policy context differ. The paper avoids spurious trend claims.

3.2 Measures

Online-recording concern. Question QB13.1 asks whether respondents are very concerned, fairly concerned, not very concerned, or not at all concerned about their behaviour being recorded on the internet, including browsing, file downloads, and access to online content. The main descriptive indicator combines "very" and "fairly" concerned. This is a general digital-recording measure. It is used as a proxy for the concern dimension of a future biometric risk disclosure, not as a direct question about biometrics.

Perceived control. Question QB6a asks respondents who had disclosed information on social-networking or sharing sites how much control they feel they have over that information, including their ability to change, delete, or correct it. Response categories are complete control, partial control, no control at all, and don't know. It captures a practical form of agency over already-disclosed personal information.

Privacy-setting action. Question QB10a asks users of social-networking or sharing sites whether they have tried to change their profile's default privacy settings. This is a behavioural indicator of active privacy management. It is not a comprehensive measure of security competence and should not be interpreted as a measure of protection against biometric leakage.

Institutional trust. Questions QB25.1–QB25.7 ask how much respondents trust different organisations to protect personal information. The analysis reports combined “totally trust” and “tend to trust” responses for national public authorities, European institutions, banks and financial institutions, health and medical institutions, internet companies, and telecommunications or internet-service providers. The contrast is substantively important: an exposure risk may be judged differently depending on whether data are held by a health provider, a bank, or a consumer internet platform.

Identity-protection practices. Question QB16 asks internet users which actions they take to protect identity online. It allows multiple answers. Selected actions include limiting unwanted email, checking transaction safety labels, using anti-spy software, deleting cookies, changing browser security settings, avoiding repeated information across sites, using a dummy email account, and asking websites to update or delete stored information. Because this is a multiple-response item, percentages are reported separately and do not sum to 100.

Awareness of identity-related problems and sensitive-data protection. Question QB30 asks whether respondents had heard about or experienced data-loss and identity-theft issues during the previous 12 months. It is also multiple response. Question QB33 asks whether genetic information such as DNA should receive the same special protection as other sensitive personal data. This measure does not concern palm-vein data directly, but it provides a public benchmark for whether body-linked information is understood as deserving special safeguards.

Country-level comparison. Country tables for QB13.1 and QB25.6 are used to compare the share concerned about online recording with the share trusting internet companies to protect personal information. EU-level aggregates and West/East Germany breakouts are excluded from this country-level comparison. Pearson's r is presented only as a descriptive ecological statistic. It cannot establish an individual-level relationship and has no causal interpretation.

3.3 Analytic strategy and transparency

The analysis proceeds in four stages. First, it summarises EU27 response distributions. Second, it presents age-group variation in concern and the distribution of perceived control and privacy-setting action among the populations to whom each question was addressed. Third, it compares trust in the

institutions responsible for personal-data protection and documents selected identity-protection practices. Fourth, it maps country-level gaps between concern and trust and reports a descriptive correlation. All percentages are taken from the official weighted tables. The analysis does not generate simulated observations, impute missing data, or construct a synthetic biometric-risk score.

Figures were produced from the downloaded official Excel tables using a reproducible script. A supporting workbook accompanies this manuscript and contains the derived table used for each chart. The manuscript applies a conservative language rule: “associated,” “co-occurs,” and “descriptive” are used for aggregate comparisons; causal language is avoided. The paper also separates findings from interpretation. The data establish the distribution of reported attitudes in 2010; the discussion considers how those attitudes might inform present-day risk communication.

3.4 Ethics and security scope

This work relies on public, de-identified, aggregate survey data and does not collect information from individuals. It does not build, test, distribute, or evaluate a side-channel method. Its discussion of palm-vein reconstruction is limited to the high-level existence of a privacy-relevant technical research context described in public scholarly records [1] [2]. Operational capabilities, device configurations, signal characteristics, reconstruction techniques, and bypass outcomes are out of scope. This boundary is not merely procedural. It keeps the paper aligned with its core contribution: understanding privacy perceptions and accountability expectations rather than enabling misuse.

4. Results

Table 1
Selected public-data indicators used in the analysis

Indicator	Percent	Item	Population
EU27 respondents concerned about online recording	40%	QB13.1	All EU27 respondents
EU27 respondents trusting internet companies	22%	QB25.6	All EU27 respondents
EU27 respondents not trusting internet companies	62%	QB25.6	All EU27 respondents
Perceived complete control over disclosed social-web information	26%	QB6a	Disclosers on social/sharing sites
Perceived no control at all	20%	QB6a	Disclosers on social/sharing sites
Changed default privacy settings	51%	QB10a	Social/sharing site users
Heard of or experienced data loss/identity theft issues	55%	QB30	All EU27 respondents; multiple response
Directly experienced data loss/identity theft issues	2%	QB30	All EU27 respondents; multiple response
Support special protection for DNA/genetic data	88%	QB33	All EU27 respondents
<i>Note. All values are weighted percentages reported in the official public tables for Special Eurobarometer 359. Question-specific populations are listed in the final column; QB30 is a multiple-response item.</i>			

4.1 Baseline concern about online recording

Figure 1 shows the EU27 distribution for concern about internet behaviour being recorded. Thirteen percent of respondents were very concerned and 27% were fairly concerned, yielding a combined concern estimate of **40%**. Twenty-three percent were not very concerned and 12% were not at all concerned. The remaining responses were 21% not applicable and 4% don't know. The sizeable not-applicable category is important. It cautions against treating 40% as a universal population estimate of concern among active internet users; the question's relevance depended on respondents' circumstances and engagement with the internet.

Even with that limitation, the result identifies a meaningful baseline of apprehension about online observation. The concern is neither marginal nor universal. It suggests a divided public environment in which a biometric privacy disclosure could be received by some as confirmation of an existing fear of data capture, while others may see the issue as remote or outside their daily experience. For communication design, this heterogeneity argues against one-size-fits-all messages. Technical notices should explain concrete implications without assuming prior knowledge or a uniform level of worry.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.

Age differences reinforce the point. As shown in Fig. 2, the combined concerned share was 41% among respondents aged 15–24, 48% among people aged 25–39, 46% among those aged 40–54, and 29% among those aged 55 or older. This pattern should not be read as a lifecycle explanation. It may reflect different forms of online engagement, differing perceived exposure, or cohort-specific digital experience. Yet it demonstrates that public concern is distributed unevenly. A provider communicating about biometric privacy should avoid assuming that younger users are automatically less concerned because they are more digitally active, or that older users are uniformly more fearful of digital systems.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.

4.2 Trust in organisations that protect personal information

The trust pattern is striking. Figure 3 shows that health and medical institutions had the highest reported trust to protect personal information at 78%, followed by national public authorities at 70%, banks and financial institutions at 62%, European institutions at 55%, telecommunications and internet-service providers at 32%, and internet companies at only **22%**. The low trust in internet companies is not a generic rejection of data holders. Respondents differentiated sharply among institution types.

This distinction matters for biometric privacy. If palm-based authentication is deployed through a health system, banking application, workplace, retail service, or platform account, the same technical disclosure may be evaluated through different institutional expectations. A provider cannot assume that a statement such as “your biometric data are secure” will have stable meaning across settings. Credibility depends on the organisation’s existing reputation and on whether its role aligns with public expectations of stewardship. High trust in health institutions also should not be interpreted as blanket permission for broad data use; it may reflect a context-specific belief that health data are sensitive and require special care.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.

4.3 Control and active adjustment of privacy settings

The data reveal a gap between having some agency and feeling fully in control. Among respondents who had disclosed information on social-networking or sharing sites, 26% reported complete control over that information, 52% reported partial control, 20% reported no control at all, and 2% did not know. The large partial-control category is meaningful. It suggests that many people may recognise some ability to change a setting or delete a profile element while still perceiving limits on their ability to manage downstream data flows.

Among social-networking or sharing-site users, 51% said they had tried to change default privacy settings, 46% had not, and 3% did not know. This distribution resists a simplistic reading. The fact that roughly half of users changed a default indicates active privacy management. The fact that almost half did not change it does not prove indifference. Default settings may be hard to understand, users may believe their current settings are sufficient, or they may face time and usability constraints. More fundamentally, a user-level settings action cannot address a risk that arises from infrastructure outside the user's control.

For the present topic, the implication is clear. A biometric side-channel concern should not be framed as another settings problem. User education may be valuable, but meaningful mitigation primarily belongs to organisations that select, operate, audit, procure, and update biometric systems. Asking individuals to protect an irreplaceable physiological characteristic without corresponding institutional safeguards creates a misleading allocation of responsibility.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.

4.4 Identity-protection practices and exposure awareness

Figure 5 shows selected online identity-protection behaviours among internet users. Forty-two percent used tools or strategies to limit unwanted email, 40% checked whether a transaction was protected or carried a safety logo or label, 39% used anti-spy software, and 35% deleted cookies. Smaller shares changed browser security settings to increase privacy (22%), avoided providing the same information to different sites (21%), used a dummy email account (12%), or asked websites to update or delete information held about them (8%).

These behaviours demonstrate effort, but they also reveal the limits of common consumer-facing privacy practices. Many actions are oriented toward visible platform interactions: email, web transactions, browser configuration, or repetitive form-filling. They do not address hidden or embedded data flows. A person who checks a safety label or deletes cookies may still have little ability to assess how a biometric acquisition device handles signals, images, templates, storage, or sharing. The gap between familiar protective habits and unfamiliar infrastructure risks is a central communication challenge.

Question QB30 provides additional context. Fifty-five percent of EU27 respondents had heard about or experienced data-loss or identity-theft issues in the previous 12 months; 42% had encountered such information through television, radio, newspapers, or the internet. Only 2% reported direct personal impact. The question allows multiple answers, so these figures cannot be combined into mutually exclusive categories. Still, the pattern suggests that public understanding of identity risk may be mediated more often by media and social awareness than by direct victimisation. Risk communication about biometric leakage should account for this. Public reactions may be shaped by narratives, examples, and institutional statements before most people have direct experience of harm.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.

The data on sensitive genetic information are also informative. Eighty-eight percent of EU27 respondents believed that genetic information such as DNA should receive at least some special protection. Palm-vein patterns are not genetic data, and the paper does not treat them as legally or scientifically identical. The comparison instead illustrates a broader normative orientation: many people expect body-linked or identity-linked information to receive safeguards that go beyond ordinary data practices. That orientation supports the view that biometric risk governance should be explicit, not assumed.

4.5 Cross-country variation and the concern–trust gap

Figure 6 compares country-level concern about online recording with country-level trust in internet companies. The gap is large in many cases. For example, concern substantially exceeded trust in Germany, France, Luxembourg, Greece, Ireland, Italy, and Austria. Other countries displayed smaller gaps or relatively higher trust. The purpose of this chart is not to rank national privacy cultures or infer stable country traits. Different media environments, regulatory histories, technologies, question interpretation, sampling variance, and the 2010 context could all influence the values. The chart simply demonstrates that public confidence cannot be treated as geographically uniform.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.

Figure 7 plots the same two measures at the country level. The Pearson correlation is small and negative ($r = -.09$, $p = .664$). This result does not show a meaningful country-level linear relationship in these public tables. It should not be transformed into an individual-level finding. A country with higher average concern is not necessarily populated by people who personally trust internet companies less, and a non-significant aggregate correlation does not imply that trust is irrelevant to individual privacy behaviour. The figure's value is methodological: concern and trust should be measured separately rather than assumed to move together.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.

5. Discussion

5.1 Interpreting the public baseline

The central finding is a pattern of concern without complete control and low trust in internet companies. Forty percent of EU27 respondents reported concern about online behaviour being recorded, yet only 26% of relevant respondents felt complete control over information they had disclosed on social or sharing sites. Meanwhile, internet companies were trusted by 22% of respondents to protect personal information, substantially below health institutions, public authorities, banks, and European institutions.

This combination suggests that a technical disclosure involving biometric leakage would not enter a neutral public environment. It would be interpreted against existing concerns about data capture and against institution-specific credibility judgments.

The finding is compatible with theories that place privacy at the intersection of risk, context, and power. A biometric system can be technically accurate and still produce public discomfort if individuals cannot understand how data move, whether a risk has been mitigated, or what recourse is available. In the language of contextual integrity, the critical issue is not simply that information exists, but whether its collection and transmission remain appropriate to the context in which the individual agreed to use the system [13]. A person consenting to palm authentication for access, payment, or service verification may expect a narrowly defined information flow. The possibility that unintended system emissions could expose additional information challenges that expectation, even if the risk is technically complex.

The study also helps explain why notification and remediation cannot be limited to technical assurances. If a provider responds to a biometric risk by telling users that the chance of harm is low, the statement may fail to address the public's core concerns. People may instead want to know whether the system will be changed, whether data are retained, whether the organisation will stop using a vulnerable configuration, who independently verified the remedy, and whether alternative authentication routes are available. These questions are fundamentally about control and institutional accountability.

5.2 Implications for risk communication

A useful disclosure about biometric privacy should be plain-language, specific about scope, and non-sensational. It should explain what category of information is at stake, which users or deployments may be affected, what the organisation has done, what remains uncertain, and how people can obtain support. It should avoid unnecessarily repeating operational details that could magnify misuse. Transparency does not require an attack manual. It requires enough information for affected people and oversight bodies to understand the relevant risk, evaluate the response, and make informed choices.

Communication should also distinguish between a biometric image, a derived template, an account identifier, and an ordinary profile attribute when that distinction is relevant to the service. People may reasonably interpret all of these as “my biometric data,” but the practical remediation options may differ. Clear statements about retention, deletion, replacement of devices, independent assessment, and alternative authentication methods matter more than generic claims of security. Acknowledging limits is preferable to overpromising. Overconfident reassurance can erode the trust that remediation depends on.

The data on protective behaviours reinforce the need for this approach. Respondents reported actions such as checking safety labels, deleting cookies, and changing browser settings. Those are understandable responses to familiar web risks. They are not meaningful levers for mitigating a risk located in acquisition hardware or institutional infrastructure. A responsible communication strategy should not imply that a user can solve a system-level biometric confidentiality problem through routine

browser hygiene. It should make clear which steps belong to the provider and which, if any, are feasible for users.

5.3 Governance and design implications

The results support a governance model based on shared but differentiated responsibility. Users should receive understandable choices and clear notices. Deployers and vendors, however, should bear the primary responsibility for secure design, procurement, validation, update management, and incident response. This aligns with the data-protection principle that sensitive processing requires safeguards proportionate to the potential impact. The GDPR treats biometric data processed for the purpose of uniquely identifying a natural person as a special category of personal data, subject to specified conditions and safeguards [18]. That legal treatment does not resolve every technical question, but it recognises that biometric processing demands heightened attention.

For organisations, four broad safeguards follow from the psychosocial evidence. First, privacy and security assessments should consider not only accuracy and spoof resistance but also data-flow confidentiality and the possibility of unintended leakage. Second, services should offer alternatives where feasible, particularly when a user has reason not to enrol a body-linked credential. Third, vulnerability communication should be coupled to auditable mitigation, such as independently reviewable remediation and meaningful redress. Fourth, organisations should avoid function creep: a biometric identifier collected for one purpose should not silently become a general identifier across unrelated contexts. Public concerns about data protection are shaped partly by the fear that information will travel farther than its original context permits [13] [14].

These principles resonate with public-attitude research. Norval and Prasopoulou [6] caution against reducing citizens to narrow “users” in a security-versus-privacy trade-off. Kugler [7] shows that people can understand biometric privacy harms as distinct and consequential. The current descriptive evidence adds a cross-national digital-privacy baseline: concern, trust, and control are separate constructs. A provider that improves only technical performance without strengthening control and institutional accountability may still face a legitimacy gap.

5.4 Limitations and future research

Several limitations are decisive. First, the Eurobarometer data were fielded in 2010. They are valuable as a public historical baseline, but they cannot estimate present-day attitudes or the current adoption of palm-vein systems. Digital platforms, data-protection law, social-media practices, and public awareness have changed substantially. Second, the questionnaire contains no item about palm-vein recognition, electromagnetic emissions, side channels, or a named technical study. The analysis therefore cannot claim that 40% of Europeans are concerned about palm-vein reconstruction, or that 22% would trust a particular biometric provider. Such statements would exceed the data.

Third, the primary analysis uses aggregate public tables. It cannot test individual-level mediation, multilevel predictors, or causal mechanisms. The country-level correlation is explicitly ecological and

non-causal. Fourth, several measures apply only to subpopulations, such as people who disclosed information on social or sharing sites, used such sites, or used the internet. Their denominators should not be generalised to all adults. Fifth, public concern is not identical to harm. A strong public reaction may be appropriate, disproportionate, or shaped by factors outside the technical severity of a particular issue. The purpose of this research is not to treat perceptions as a substitute for security assessment.

Future work should therefore use a preregistered, scenario-based survey that directly names a palm-based biometric authentication context in non-technical language. It could experimentally vary three transparent factors: the service context, the type of institutional response, and the degree of user control offered after disclosure. Outcome measures should distinguish perceived severity, perceived likelihood, trust, willingness to use the system, support for regulation, and preferences for alternatives. Qualitative interviews could further explore whether people see vascular biometrics as closer to passwords, health data, identifiers, or something else. Any such work should undergo ethical review, avoid providing operational attack detail, and include participants with differing levels of digital access and experience.

6. Conclusion

A biometric side-channel risk is not solely an engineering event. It is also a challenge of trust, understanding, responsibility, and control. This public-data analysis does not measure reactions to palm-vein reconstruction directly, and it does not attempt to reproduce a technical vulnerability. It shows instead that the broader EU27 baseline in 2010 contained substantial concern about online recording, low trust in internet companies, incomplete perceived control over disclosed information, and uneven engagement in identity-protection practices. These conditions suggest that biometric privacy risks should be governed and communicated as institutional accountability problems, not as user-hygiene problems. Technical remediation is necessary. Public legitimacy depends on whether people can see that safeguards are real, proportionate, and responsive to the distinctive stakes of body-linked data.

Declarations

Competing Interests

The authors declare no competing interests.

Ethics Approval and Consent to Participate

Not applicable. This study is a secondary analysis of publicly available, de-identified aggregate data and involved no human-participant recruitment or access to individual-level records.

Author Contributions

Lu Ziwen: Conceptualization, methodology, formal analysis, visualization, writing—original draft, and correspondence. Hu P. F. and Gao X.: Writing—review and editing. All authors reviewed and approved the final manuscript.

Data Availability and Reproducibility Statement

All quantitative results are derived from the public tables for Special Eurobarometer 359, Attitudes on Data Protection and Electronic Identity in the European Union, available through the official EU data portal (https://data.europa.eu/data/datasets/s864_74_3_ebs359?locale=en). The derived values used for the figures are supplied in `public_data_analysis_tables.xlsx`; all figures are embedded in this manuscript. No simulated observations were created. The analysis is descriptive and uses the exact public-table denominators reported in figure notes.

References

1. Lu Z, Gao X, Gao N, Zhang G, Cao Y, Spolaor R, Yang Y, Cheng X, Hu P (2026) Palm vein reconstruction from electromagnetic side-channel emissions. **IEEE Trans Mob Computing** 25:14270–14283. <https://doi.org/10.1109/TMC.2026.3677817>
2. Xu H, Zhao T, Wang X, Ma L, Dai J, Wyglinski A, Sun X et al (2026) EMPalm: Exfiltrating palm biometric data via electromagnetic side-channel. In **Proceedings of the 2026 ACM/IEEE International Conference on Embedded Artificial Intelligence and Sensing Systems** (pp. 1043–1056). <https://doi.org/10.1145/3774906.3802764>
3. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. **IEEE Trans Circuits Syst Video Technol** 14(1):4–20. <https://doi.org/10.1109/TCSVT.2003.818349>
4. Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. **IBM Syst J** 40(3):614–634. <https://doi.org/10.1147/sj.403.0614>
5. Campisi P (ed) (2013) Security and privacy in biometrics. Springer. <https://doi.org/10.1007/978-1-4471-5230-9>
6. Norval AJ, Prasopoulou E (2019) Seeing like a citizen: Exploring public views of biometrics. **Political Studies**, 67*(2), 367–387. <https://doi.org/10.1177/0032321718766736>
7. Kugler MB (2019) From identification to identity theft: Public perceptions of biometric privacy harms. **UC Irvine Law Rev** 10*, 107–145. <https://escholarship.org/uc/item/7ns62279>
8. Zhang W, Zhang H, Deng Z (2025) Public attitude and media governance of biometric information dissemination in the era of digital intelligence. **Scientific Rep** 15* Article 2600. <https://doi.org/10.1038/s41598-025-86603-w>
9. Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and human behavior in the age of information. **Science**, 347*(6221). 509–514. <https://doi.org/10.1126/science.aaa1465>

10. Smith HJ, Dinev T, Xu H (2011) Information privacy research: An interdisciplinary review. *MIS Q* 35(4):989–A27. <https://doi.org/10.2307/41409970>
11. Malhotra NK, Kim SS, Agarwal J (2004) Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. **Information Syst Res* 15(4):336–355. <https://doi.org/10.1287/isre.1040.0032>
12. Dinev T, Hart P (2006) Internet privacy concerns and social awareness as determinants of intention to transact. **International J Electron Commer* 10* 27–29. <https://doi.org/10.2753/JEC1086-4415100201>
13. Nissenbaum H (2004) Privacy as contextual integrity. **Washington Law Review*, 79*, 119–158. <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/>
14. Solove DJ (2006) A taxonomy of privacy. **University Pa Law Rev* 154* (3), 477–560. https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/
15. Taddicken M (2014) The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. **Journal of Computer-Mediated Communication*, 19*(2), 248–273. <https://doi.org/10.1111/jcc4.12052>
16. European Commission (2010) **Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union** [Public data tables]. Publications Office of the European Union. https://data.europa.eu/data/datasets/s864_74_3_ebs359?locale=en
17. European Commission (2017) Eurobarometer 83.1: Europeans in 2015, Data Protection and the Internet, February–March 2015. Ann Arbor, MI: GESIS [distributor], Inter-university Consortium for Political and Social Research [distributor]. <https://doi.org/10.3886/ICPSR36665.v1>
18. European Parliament and Council of the European Union (2016) Regulation (EU) 2016/679 (General Data Protection Regulation). **Official J Eur Union* L119*, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Figures

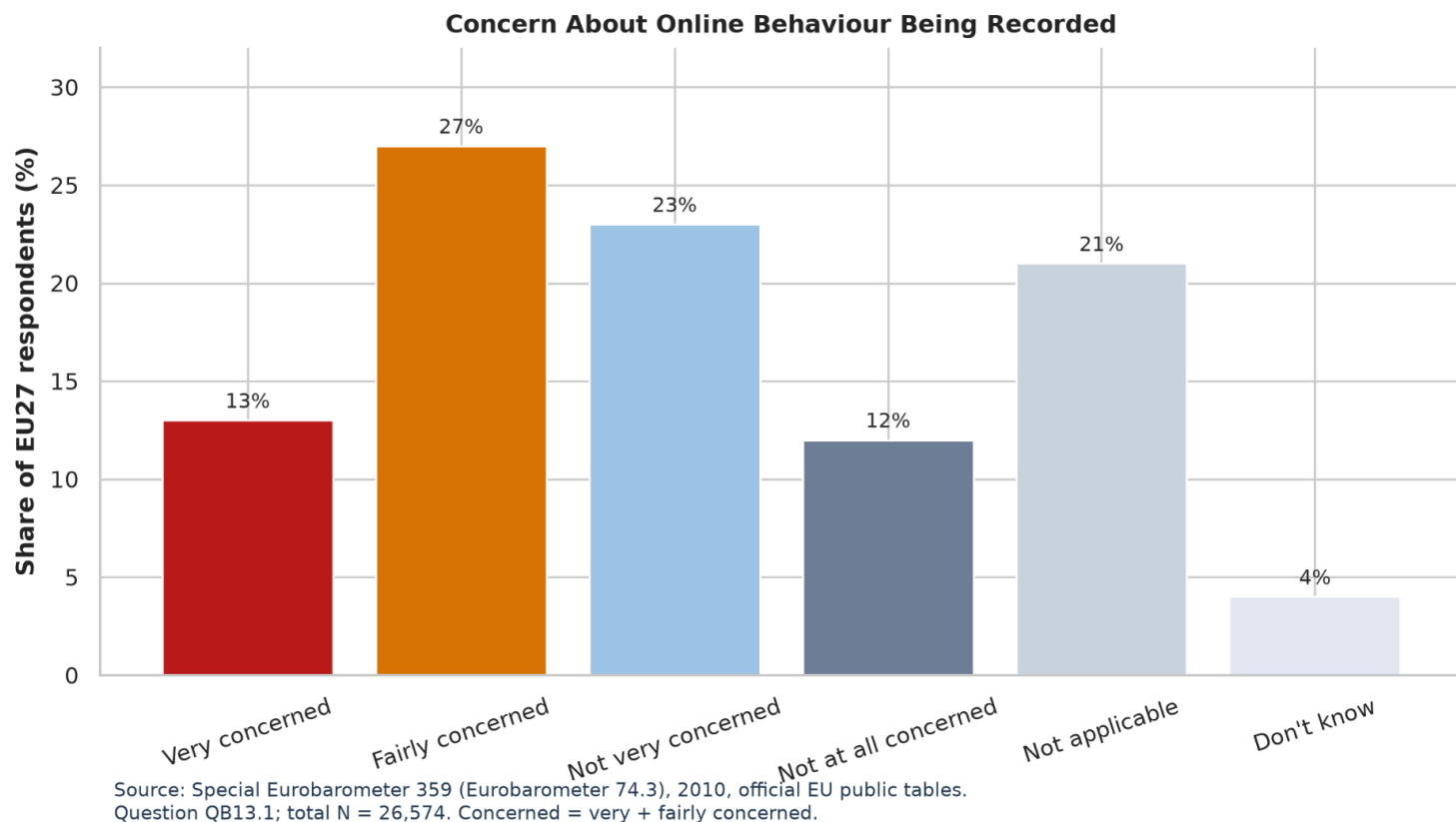
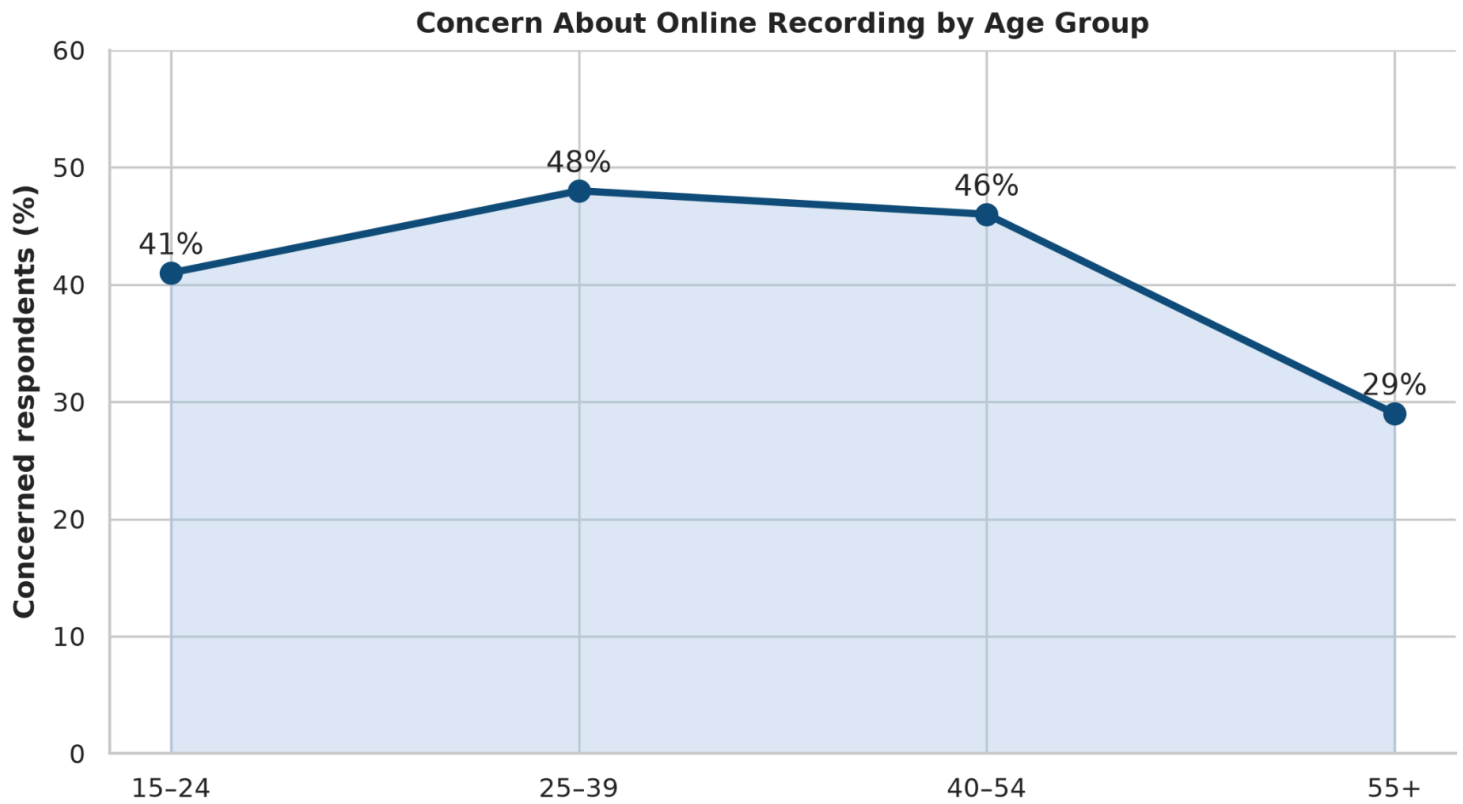


Figure 1

Concern about online behaviour being recorded in the EU27.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.



Source: Special Eurobarometer 359 (Eurobarometer 74.3), 2010, official EU public tables.
QB13.1; concerned = very + fairly concerned; unweighted public table percentages displayed by age.

Figure 2

Concern about online recording by age group.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.

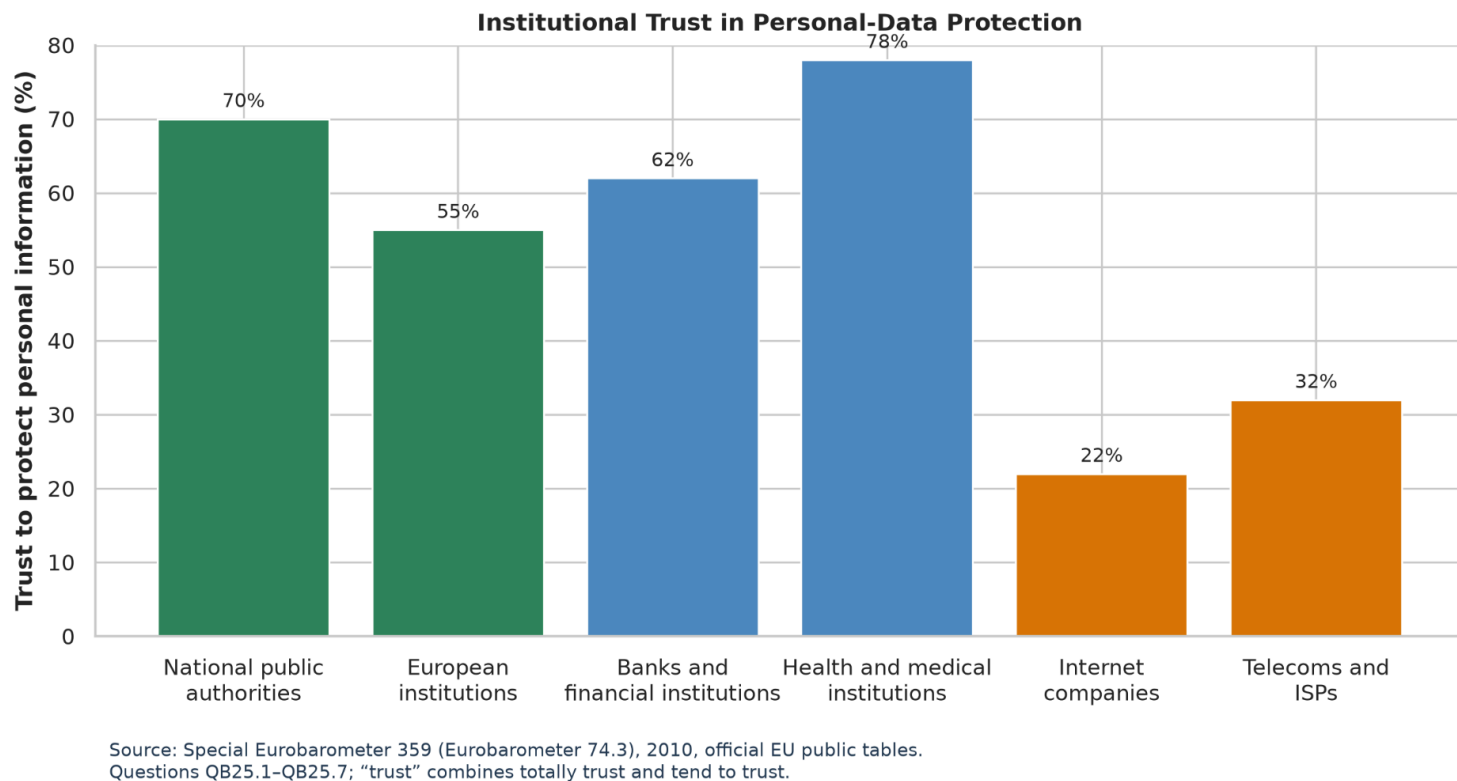
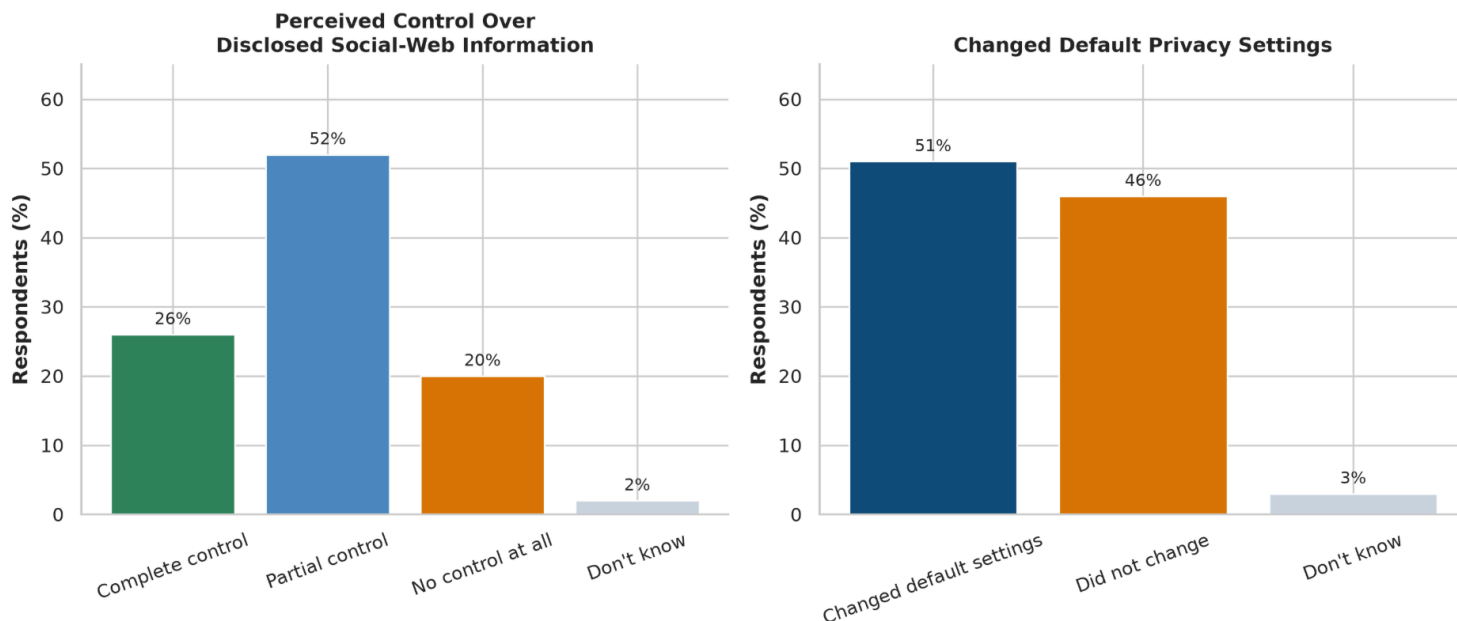


Figure 3

Institutional trust in personal-data protection.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.



Source: Special Eurobarometer 359 (Eurobarometer 74.3), 2010, official EU public tables. QB6a respondents had disclosed information on social/sharing sites (N = 9,582); QB10a respondents used such sites (N = 10,560).

Figure 4

Perceived control over disclosed information and changes to default privacy settings.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.

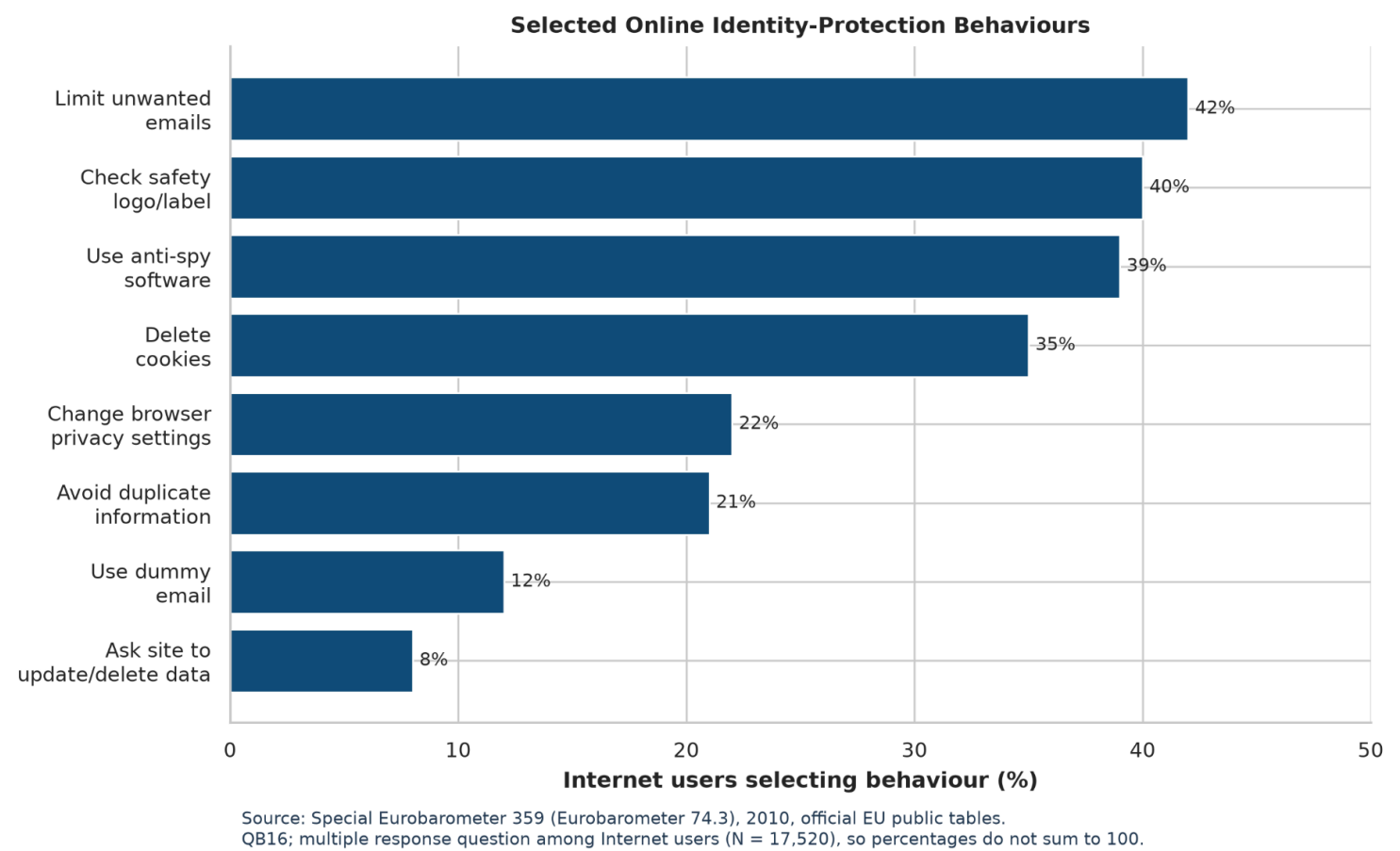


Figure 5

Selected online identity-protection behaviours.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.

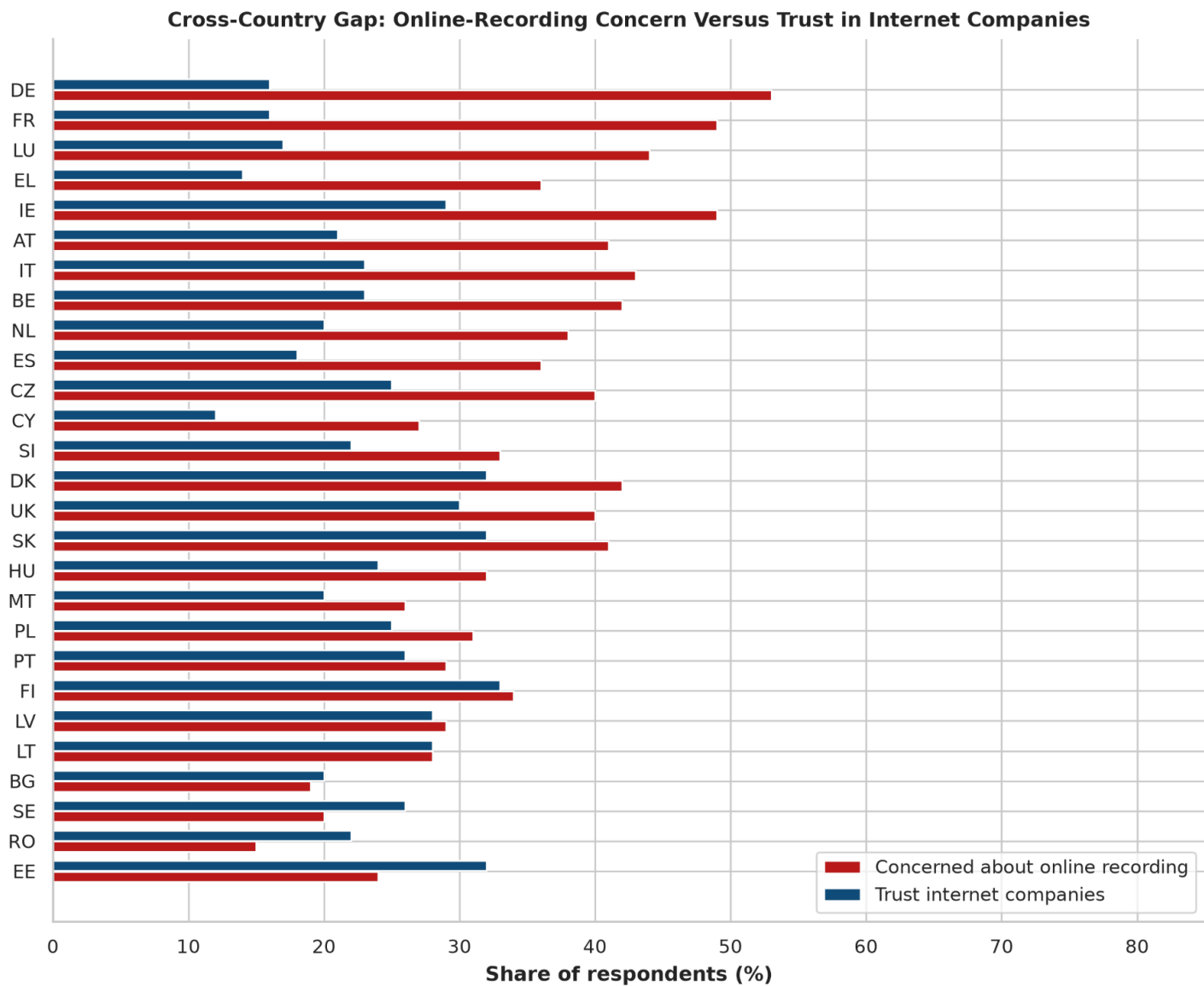
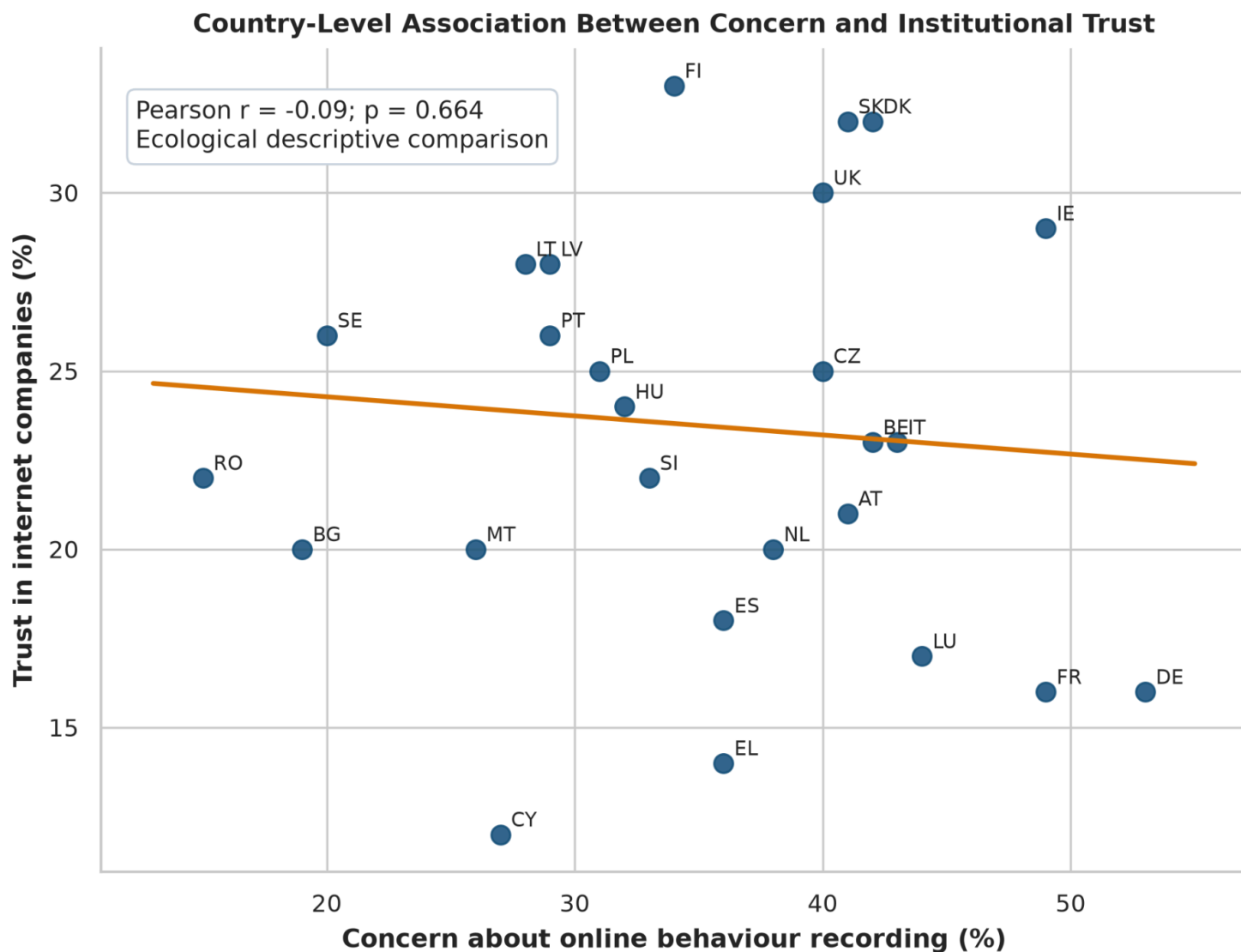


Figure 6

Cross-country gap between online-recording concern and trust in internet companies.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.



Source: Special Eurobarometer 359 (Eurobarometer 74.3), 2010, official EU public tables.
Unit = country aggregate; this figure is not an individual-level association and does not support causal inference.

Figure 7

Country-level association between concern and trust in internet companies.

Source note: Special Eurobarometer 359 (Eurobarometer 74.3), official public tables. Full sample, question, denominator, and aggregation details are printed in the figure itself and described in the Method section.