Sabro E, Torralbo Muñoz B, 'Redefining "reasonable harm" to privacy in the digital surveillance era: a critical analysis of israeli legal framework' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252SETMB

EJPLT
ISSN 2704-8012

Redefining "reasonable harm" to privacy in the digital surveillance era: a critical analysis of israeli legal framework

Ridefinire il 'danno ragionevole' alla privacy nell'era della sorveglianza digitale: un'analisi critica del quadro giuridico israeliano

EYAL SABRO
Lawyer, Privacy consultant & DPO
University of Cordoba

BARTOLOMÉ TORRALBO MUÑOZ
Assistant Professor, Ph.D. in Criminal Law
University of Cordoba

Abstract

This article examines the concept of "reasonable harm" to privacy in the context of digital surveillance, focusing on Israel's legal framework. It analyzes tensions between formal legal definitions and public perceptions of privacy violations, revealing significant gaps that complicate the establishment of coherent standards. The Israeli case demonstrates how traditional spatial conceptions of privacy are increasingly inadequate in digital environments where information flows transcend physical boundaries. Empirical research highlights the "privacy paradox" in Israeli society – the discrepancy between expressed privacy concerns and actual privacy-protective behaviors. The article proposes new legal tests for evaluating privacy violations that incorporate considerations of chilling effects, contextual integrity, proportionality, and procedural safeguards. By developing more nuanced approaches to these questions, democracies can work toward a future where security and privacy are recognized as complementary rather than competing values.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
Questo articolo esamina il concetto di "danno ragionevole" alla privacy nel contesto della sorveglianza digitale, concentrandosi sul quadro giuridico israeliano. Analizza le tensioni tra definizioni legali formali e percezioni pubbliche delle violazioni della privacy, rivelando lacune significative che complicano la definizione di standard coerenti. Il caso israeliano dimostra come le concezioni spaziali tradizionali della privacy siano sempre più inadeguate negli ambienti digitali dove i flussi di informazioni trascendono i confini fisici. La ricerca empirica evidenzia il "paradosso della privacy" nella società israeliana – la discrepanza tra preoccupazioni espresse sulla privacy e comportamenti effettivi di protezione. L'articolo propone nuovi test legali per valutare le violazioni della privacy che incorporano considerazioni sugli effetti inibitori, l'integrità contestuale, la proporzionalità e le salvaguardie procedurali. Sviluppando approcci più sfumati a queste questioni, le democrazie possono lavorare verso un futuro in cui sicurezza e privacy sono riconosciute come valori complementari piuttosto che competitivi.

Keywords: privacy; digital surveillance; reasonable harm; Israeli law; proportionality; contextual integrity

Summary: 1. Introduction: The Dialectic of Privacy and Security in Modern Surveillance. – 2. Theoretical Framework: Evolving Privacy Conceptions in a Digital Landscape. – 2.1. The Epistemological Crisis of "Reasonable Harm" in the Digital Surveillance Era. – 2.2. From Spatial to Contextual Understanding of Privacy. – 2.3. Privacy and Security in Democratic Societies. – 2.4. The Chilling Effect and Democratic Participation. – 3. The Israeli Legal Framework for Digital Privacy and Surveillance. – 3.1. Constitutional Protection of Privacy. – 3.2. The Privacy Protection Law and Its Implementation. – 3.3. Wiretapping and Communications Data Laws. – 3.4. Recent Legislative Developments: The Spyware Law. – 3.5. Judicial Interpretation of Privacy in Surveillance Contexts. – 3.6. The Constitutional Paradox: Fundamental Rights with Structural Immunity. – 4. The Gap Between Legal Definitions and Public Perceptions. – 4.1. Empirical Evidence of Public Privacy Concerns. – 4.2. The Privacy Paradox in Israeli Society. – 4.3. The Enforcement Gap. – 4.3.1 Case Study: The Enforcement Gap as Epistemic Crisis. – 5. Developing New Legal Tests for "Reasonable Harm". – 5.1 The Chilling Effect Test. – 5.2. The Contextual Integrity Framework. – 5.3 The Proportionality Requirement. – 5.4 The Independent Oversight Mechanisms. – 6. Conclusion: Reimagining Privacy Protections in an Era of Pervasive Surveillance.

1. Introduction: The Dialectic of Privacy and Security in Modern Surveillance.

The fundamental question of what constitutes "reasonable harm" to privacy in an era of pervasive digital surveillance has emerged as one of the most challenging legal dilemmas faced by modern democracies. As digital technologies increasingly permeate daily life, the capacity for surveillance by state entities and private actors alike has expanded exponentially, creating unprecedented tensions between security imperatives and privacy rights. This

dialectic is particularly pronounced in Israel, where a unique confluence of security concerns, democratic values, and rapid technological innovation has created a complex legal landscape for privacy protection.

The core research question this article addresses is how to define "reasonable harm" to privacy from a legal perspective in an era of extensive digital surveillance. Specifically, what tensions exist between formal legal definitions of harm and public perceptions of privacy violations? How have Israeli courts interpreted this concept, and what new legal tests might better balance the competing interests at stake?

Israel presents a particularly compelling case study for examining these questions. As a democracy facing persistent security challenges, Israel has developed sophisticated surveillance capabilities while maintaining a commitment to democratic principles and the protection of fundamental rights. This tension has led to a distinctive body of case law and legislation that reflects broader global challenges in reconciling privacy and security interests. The Israeli Basic Law: Human Dignity and Liberty (1992) provides constitutional protection for privacy, yet security exceptions and expansive surveillance authorities create a complex regulatory environment.

The relevance of this inquiry extends beyond Israeli borders. As Heikkilä argues, "the challenge of reconciling surveillance imperatives with privacy protection is fundamental to modern democratic governance worldwide".[1] This challenge has only intensified following Edward Snowden's revelations about mass surveillance programs, which sparked global debates about the permissible boundaries of state monitoring.[2]

By exploring these questions, this article contributes to both scholarly debates and practical policy discussions about privacy protection in the digital age. It argues that traditional conceptions of privacy harm are inadequate for addressing the novel challenges posed by modern surveillance technologies, and that new frameworks incorporating elements of contextual integrity, proportionality, and transparent oversight are needed to ensure meaningful privacy protection while accommodating legitimate security interests.

2. Theoretical Framework: Evolving Privacy Conceptions in a Digital Landscape.

2.1 The Epistemological Crisis of "Reasonable Harm" in the Digital Surveillance Era.

In contemporary privacy law, the dominant harm-based approach typically requires that claimants demonstrate a cognizable, "reasonable" or "reasonably foreseeable" harm as a precondition for legal intervention. Under this standard, courts and regulators are expected to translate diffuse privacy concerns into concrete, individualized injuries that can be recognised,

[1] H Heikkilä, 'Beyond Moral Coupling: Analysing Politics of Privacy in the Era of Surveillance' (2020) 8 Media and Communication 248, 250.
[2] N Ni Loideain, 'EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era' (2015) 3 Media and Communication 53, 54.

measured, and remedied on a case-by-case basis, while filtering out speculative, abstract, or purely dignitary interests.[3]

Against this background, before delving deeper into evolving privacy conceptions, we must confront a fundamental conceptual crisis: the very definition of “reasonable harm” as an appropriate legal framework for evaluating privacy violations in the digital age.

The problem is not merely practical, that is, difficulties in measuring or quantifying intangible harms, but substantive: the harm paradigm relies on a dichotomy between a normative baseline state and a measurable deviation from it. As Solove and Citron demonstrate, legal doctrines built around concrete, individualized injury struggle to accommodate the diffuse, cumulative, and often intangible nature of contemporary privacy harms.[4] However, in the context of digital surveillance, the very architecture of monitoring and collection creates a new reality of "surveillance normalization”[5] in which the concept of "harm" as a deviation from a norm becomes incoherent.[6] As evident from an examination of Israeli jurisprudence, courts are forced to retroactively invent indicators for "harm" that were not theoretically developed in the first place, thereby producing a legal fiction that masks the concept's inadequacy to technological reality. In practice, the reasonable harm threshold enables courts and regulators to translate diffuse privacy concerns into discrete, litigable injuries that can be recognized, measured, and remedied on a case-by-case basis.

The legal fiction of "reasonable harm" allows courts to adjudicate concrete cases while creating an illusion of doctrinal continuity. Still, it conceals the deeper failure: our inability to conceptualize privacy infringement in the digital surveillance era in terms of singular, measurable, and immediate "harm." The fundamental question, then, is not merely what constitutes "reasonable harm," but whether the very use of the harm paradigm remains effective or has become anachronistic in an era where the potential for privacy violations is structural, persistent, and often invisible. As Parsons argues, pervasive mass surveillance erodes the communicative conditions of democracy itself, producing harms that are structural and societal rather than discrete and individualized.[7]

---

[3] DJ Solove, DK Citron, ‘Privacy Harms’ (2022) 102 Boston University Law Review 793; Office of Information Policy, ‘OIP Guidance: Applying a Presumption of Openness and the Foreseeable Harm Standard’ (US Department of Justice, 3 September 2024); ‘Foreseeable Harm Standard’ (FOIA Wiki, 2025).

[4] See ibid (2022) 102 Boston University Law Review 793.

[5] LK Donohue, ‘Surveillance Normalization’ (2023) *Harvard Civil Rights-Civil Liberties Law Review* (forthcoming). See also D Mac Síthigh and A Murschetz, ‘The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates after the Snowden Revelations’ (2017) International Journal of Communication 11.

[6] E Selinger, JH Rhee, ‘Normalizing Surveillance’ (2021) 22(1) Nordic Journal of Applied Ethics 49.

[7] C Parsons, ‘Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance’ (2015) 3 Media and Communication 1.

2.2 From Spatial to Contextual Understanding of Privacy.

The inadequacy of spatial metaphors for understanding privacy in digital contexts has led scholars to develop more nuanced theoretical frameworks. Nissenbaum's theory of contextual integrity offers a particularly valuable approach, suggesting that privacy violations occur not simply when information moves from a "private" to a "public" sphere, but when information flows transgresses contextual norms governing the appropriate collection, use, and dissemination of information.[8]

In the Israeli context, this evolution from spatial to contextual understanding of privacy is evident in case law. In Ploni v The Regional Rabbinical Court in Netanya (HCJ 6650/04), the Supreme Court recognized that privacy rights can exist even in shared spaces, holding that filming a spouse in their shared home without consent constitutes a privacy violation. The Court emphasised that the decisive question is not the formal status of the space (private or shared), but the nature of the relationship between the parties and the reasonable expectations of privacy that arise within it, particularly in intimate and vulnerable settings such as the home. In doing so, the Court signaled a move away from a rigid spatial conception of privacy toward a contextual approach that evaluates how surveillance practices disrupt trust, autonomy, and legitimate expectations within specific social relationships.

This represents a significant shift from purely spatial conceptions of privacy toward a more contextual understanding that considers relationship dynamics and reasonable expectations in a specific situation.[9]

2.3 Privacy and Security in Democratic Societies.

The theoretical foundation for balancing privacy and security interests in democratic societies typically draws on principles of proportionality, necessity, and transparent oversight. The proportionality principle, which features prominently in Israeli constitutional jurisprudence, requires that any infringement of fundamental rights be proportionate to the legitimate aim pursued. As Barak has shown, proportionality in the Israeli context is structured as a four-stage test, requiring a proper purpose, a rational connection between means and end, use of the least restrictive means, and a final balancing between the benefit of the measure and the harm to the right.[10]

This principle provides a framework for assessing whether surveillance measures that impinge on privacy constitute "reasonable harm" or cross the threshold into disproportionate violations, as articulated through the three-stage proportionality test developed under the limitations clause of Basic Law: Human Dignity and Liberty.[11]

---

[8] H Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119, 136-38.
[9] HCJ 6650/04 *Ploni v. The Regional Rabbinical Court in Netanya* [2006] unpublished.
[10] Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge University Press 2012).
[11] CA 6821/93 United Mizrahi Bank Ltd v Migdal Cooperative Village IsrSC 49(4) 221; see also 'Israel's Basic Law on Human Dignity and Liberty, 1992' (Palestine Open Maps, 2011) (describing the limitations clause as a proportionality test composed of rational connection, least restrictive means and balancing).

2.4 The Chilling Effect and Democratic Participation.

A crucial theoretical dimension of privacy harm in surveillance contexts concerns what has been termed the "chilling effect," the tendency for surveillance to inhibit lawful activities, free expression, and democratic participation. As Zuboff argues, surveillance can fundamentally alter behavior and undermine autonomy, even without direct coercion. This dimension of harm extends beyond individual privacy violations to implicate broader democratic values.[12]

In that matter, at the beginning of the 20th century, Richards already contended that surveillance itself must be recognised as a constitutional harm, given its chilling effects on intellectual privacy and its distortion of power relations between watcher and watched, even in the absence of demonstrable, event-like injury.[13]

Research in Israel has empirically demonstrated this effect. A 2020 study by the Heinrich Böll Foundation found that awareness of governmental surveillance led to behavioural modifications among Israeli citizens, with 41% of Arabic-speaking respondents and 29% of Hebrew-speaking respondents expressing concerns about digital monitoring.[14]

3. The Israeli Legal Framework for Digital Privacy and Surveillance.

3.1 Constitutional Protection of Privacy.

Unlike many Western democracies, Israel lacks a formal written constitution. Instead, a series of Basic Laws serves as the constitutional cornerstone, with the Basic Law: Human Dignity and Liberty (1992) providing the constitutional foundation for privacy protection. Article 7 of this Basic Law states, "All persons have the right to privacy and intimacy," and specifically prohibits searches of a person's private premises, body, or possessions, as well as the violation of a person's privacy in conversations, writings, or records.[15]

Privacy enjoys a privileged status in Israel's constitutional hierarchy as one of the few rights explicitly enumerated in the Basic Law. However, like other constitutional rights in Israel, privacy protection is not absolute. Article 8 of the Basic Law establishes that rights may be infringed by laws "befitting the values of the State of Israel, enacted for a proper purpose, and to an extent no greater than is required". [16] This proportionality clause provides the constitutional foundation for balancing privacy against competing interests, particularly security concerns. This requirement is anchored in the "limitations clause" of

---

[12] Zuboff shows how surveillance capitalism shifts from merely predicting behaviour to systematically modifying it, thereby eroding individual autonomy even in the absence of overt coercion. See S Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).

[13] NM Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934.

[14] Heinrich Böll Foundation, 'Invisible Surveillance, Indifferent Publics: Israeli Perceptions of Surveillance (2020) <https://il.boell.org/sites/default/files/2020-11/Invisible-Surveillance-Indifferent-Publics-Israeli-Perceptions.pdf> accessed 20 March 2023.

[15] Basic Law: Human Dignity and Liberty, 5752-1992, SH No. 1391, 150, art 7.

[16] ibid art 8.

Basic Law: Human Dignity and Liberty, which permits infringements of constitutional rights only when they serve a proper purpose and are limited "to an extent no greater than is required".[17]

3.2 The Privacy Protection Law and Its Implementation.

The Privacy Protection Law (1981) predates the Basic Law but serves as the primary legislative framework governing privacy in Israel. Section 2 of the Law defines privacy violations to include various forms of surveillance, such as "spying on or trailing a person in a manner likely to harass them, or any other harassment," as well as "photographing a person while they are in a private domain," and "the violation of the duty of confidentiality prescribed by law regarding a person's private affairs".[18]

Notably, the Privacy Protection Law includes exemptions for security authorities under Section 19(b), which states that "a security authority or a person employed by it or acting on its behalf shall bear no responsibility under this Law for an infringement reasonably committed within the scope of their functions and for performance thereof". This provision effectively grants security authorities broad immunity from civil liability under the Privacy Protection Law for surveillance activities carried out within the scope of their official duties, so long as those activities can be justified as "reasonably" connected to their mandated functions.[19]

Empirical analysis of judicial decisions under the Privacy Protection Law reveals interesting patterns in its implementation. A study examining a decade of Israeli judicial decisions on data protection (2012-2022) found that civil lawsuits for privacy violations constitute a negligible share of all civil proceedings in Israel.[20] The most common ground for civil lawsuits under the Privacy Protection Law is "spying on or tracing a person", which appears in 36.9% of civil court rulings.[21] However, claims related to privacy violations in databases, a critical area in the context of digital surveillance, were virtually non-existent in civil lawsuits, suggesting potential gaps in enforcement or public awareness.

3.3 Wiretapping and Communications Data Laws.

Israel's legal framework for communications surveillance is primarily governed by two key laws: the Wiretap Law (1979) and the Communications Data Law (2007). These laws establish the conditions under which state authorities may intercept communications or access communications metadata.

The Wiretap Law permits wiretapping for national security purposes with ministerial authorization, while law enforcement wiretapping requires judicial

[17] Basic Law: Human Dignity and Liberty 5752-1992, s 8.
[18] Privacy Protection Law, 5741-1981, SH No. 1011, 128, s 2.
[19] ibid s 19(b).
[20] R Dvash, 'Analysis of a Decade of Israeli Judicial Decisions Related to Data Protection (2012-2022)' (Future of Privacy Forum, 27 April 2023) <https://fpf.org/blog/analysis-of-a-decade-of-israeli-judicial-decisions-related-to-data-protection-2012-2022/> accessed 1 April 2023.
[21] ibid.

approval. Although this dual-track system attempts to balance security needs with privacy protections, critics have noted that it creates significant disparities in oversight. As Cahane observes, "The procedural and substantive safeguards in place for security wiretapping are weaker than those for law enforcement wiretapping, raising concerns about adequate protection against disproportionate surveillance".[22]

The Communications Data Law authorizes law enforcement agencies to obtain communications metadata from service providers for investigation, detection, and prevention of crime. The law requires judicial approval for metadata requests, except in urgent cases. However, it does not apply similar restrictions to intelligence agencies accessing the same data. This discrepancy in treatment has been criticized as creating a significant loophole in privacy protection.

3.4 Recent Legislative Developments: The Spyware Law.

In November 2024, the Israeli Knesset preliminarily approved the controversial Bill on Police Access to Computer Material (commonly referred to as the "Spyware Law"),[23] which would grant the police expanded surveillance powers.[1] The proposed law would authorize the use of court-approved surveillance technology for serious offenses punishable by ten years or more in prison, where covert searches are crucial to investigating and preventing criminal acts effectively.[24]

The Spyware Law has faced significant criticism from both the Public Defender's Office and the Attorney General, who argue that it represents "a severe blow to the rule of law" and would create a "severe violation of the constitutional right to privacy". [25] Particularly controversial is the law's exclusion of public corruption offenses from its scope, which critics argue could shield government officials from accountability.

3.5 Judicial Interpretation of Privacy in Surveillance Contexts.

Israeli courts have developed a significant body of case law interpreting privacy rights in the context of surveillance. A key concept that has emerged is the "reasonable expectation of privacy" test, which evaluates whether an individual can reasonably expect privacy in a specific situation. This test was articulated in Ploni v The Regional Rabbinical Court in Netanya (HCJ 6650/04), where the Supreme Court held that filming a spouse in their shared home without consent constitutes a privacy violation, even though the space was shared.[1] The Court stressed that the existence of privacy does not depend

[22] A Cahane, 'Regulation of Online Surveillance in Israeli Law and Comparative Law' (Israel Democracy Institute, January 2019) 233.
[23] See eg, P Cohen, 'Israeli Government Advances "Spyware Law" Without Anti-Bribery Clause' (1 December 2024) <https://www.pearlcohen.com/israeli-government-advances-spyware-law-without-anti-bribery-clause/> (linking to the full text of the Bill on Police Access to Computer Material in Hebrew). Also see T Hilaie, 'The "Spyware Law" Passed Preliminary Approval, The Opposition Boycotted' (13 November 2024).
[24] T Hilaie, 'The "Spyware Law" Passed Preliminary Approval, The Opposition Boycotted' (13 November 2024).
[25] T Zimuki, 'The Attorney General Opposes a Law Advanced by the Coalition: Demands Spyware Use Also in Cases of Government Corruption' (31 October 2024).

solely on the formal classification of a space as “private” or “public”, but on the nature of the relationship and the legitimate expectations of privacy that arise within it, particularly in intimate settings such as the home.[26]

In Fisher v. State of Israel (2021), the National Labor Court established important precedents regarding workplace surveillance, ruling that employers must obtain explicit written consent for monitoring employees' emails or digital activities and must minimize privacy infringements to the absolute minimum necessary.[27] This decision reflects a growing judicial recognition of the need for explicit consent and proportionality in digital surveillance contexts.

The courts have also addressed the use of advanced surveillance technologies. In Orich v. State of Israel (2023), the court established a precedent that searching mobile devices without a detailed judicial warrant constitutes a disproportionate invasion of privacy, calling for legislative updates to regulate the use of advanced surveillance technologies.[28]

3.6 The Constitutional Paradox: Fundamental Rights with Structural Immunity.

A deeper analysis of the Israeli legal system reveals a substantive paradox that undermines privacy protection: on one hand, the Basic Law: Human Dignity and Liberty provides constitutional protection for privacy, while on the other hand, Section 19(b) of the Privacy Protection Law grants broad exemptions to security authorities acting "within the scope of their functions”. This paradox raises a penetrating question: can privacy be genuinely considered a fundamental right when the entities with the most tremendous potential to infringe upon it enjoy structural immunity? This contradiction becomes more acute in light of statistics showing that 99.3% of wiretap requests were approved in 2021. This figure suggests that judicial review, which should ensure proportionality, has become an almost automatic approval mechanism, effectively emptying procedural protections of substantive content. This situation compels us to question whether the constitutional doctrine of proportionality, which the court relies upon so heavily, has become a mere rhetorical device that legitimizes rather than constrains state surveillance.

The structural contradictions within the Israeli legal framework exemplify what legal philosopher Gunther Teubner identifies as "constitutional moments": instances in which the internal logic of a legal system confronts its limitations. [29] In the case of privacy protection, the Israeli legal system simultaneously affirms privacy as a constitutional right while systematically undermining its enforceability against the state's most powerful surveillance actors. This is not merely a technical inconsistency but reveals a more profound epistemic crisis in privacy law's ability to conceptualize harm in the surveillance context.

---

[26] HCJ 6650/04 Ploni v The Regional Rabbinical Court in Netanya (unpublished).
[27] National Labor Court Case 90/08 *Isakov v. State of Israel* [2021].
[28] *Orich v. State of Israel [2023].*
[29] G Teubner, ‘A Constitutional Moment? The Logics of “Hitting the Bottom”’ in PF Kjaer, G Teubner and A Febbrajo (eds.) *The Financial Crisis in Constitutional Perspective: The Dark Side of Functional Differentiation* (Hart Publishing 2011).

4. The Gap Between Legal Definitions and Public Perceptions.

A critical dimension in analyzing what constitutes "reasonable harm" to privacy is understanding the gap between formal legal definitions and how the public perceives and experiences privacy violations.

4.1 Empirical Evidence of Public Privacy Concerns.

Empirical research on privacy perceptions in Israel reveals complex and sometimes contradictory public attitudes. A 2020 study by the Heinrich Böll Foundation found significant levels of unawareness and indifference regarding state surveillance programs: 41% of Arabic-speaking respondents and 29% of Hebrew-speaking respondents were unaware of mass surveillance of cellular data for COVID-19 contact tracing, while 54% of Jewish respondents and 65% of Arab respondents expressed indifference or hesitation about the surveillance's implications for their privacy.[30]

This relative indifference contrasts with heightened concerns in specific contexts. Research on social media privacy in Israel has found that, despite awareness of privacy risks, 82% of Israeli users continue to share personal information online, exhibiting what researchers term "selective awareness," recognizing privacy risks while believing they primarily affect others rather than themselves.[31] This disconnect between abstract privacy concerns and actual behavior creates significant challenges for determining what constitutes "reasonable" privacy expectations in legal contexts.

4.2 The Privacy Paradox in Israeli Society.

The discrepancy between expressed privacy concerns and actual privacy-protective behaviors, often referred to as the "privacy paradox," is particularly pronounced in Israeli society. The discrepancy between expressed privacy concerns and actual privacy-protective behaviors, often referred to as the “privacy paradox”, is particularly pronounced in Israeli society.[32]

Annual surveys by the Israel Democracy Institute (2015-2017) revealed that 68% of Israelis are willing to sacrifice privacy for improved personal security.[33] At the same time, 57% expressed concerns about the potential misuse of biometric data by authorities, despite a majority supporting the implementation of biometric technologies for security purposes.[34]

---

[30] Heinrich Böll Foundation, 'Invisible Surveillance, Indifferent Publics: Israeli Perceptions of Surveillance' (2020) <https://il.boell.org/sites/default/files/2020-11/Invisible-Surveillance-Indifferent-Publics-Israeli-Perceptions.pdf> accessed 20 March 2023.

[31] 'Privacy in New Media in Israel: How Social Networks are Helping to Shape the Perception of Privacy in Israeli Society' (2018) 17 Journal of Media Studies 203, 211-15.

[32] Y Karniel and A Lavie-Dinur, ‘Privacy in New Media in Israel: How Social Networks Are Helping to Shape the Perception of Privacy in Israeli Society’ (2018) 17 Journal of Media Studies 203 (identifying a marked gap between Israeli users’ awareness of online privacy risks and their continued willingness to share personal information online); Israel Democracy Institute, ‘Privacy in a Digital World’ (2019) <https://en.idi.org.il/articles/28743> (describing the “privacy paradox” as a central feature of Israelis’ digital behaviour).

[33] Israel Democracy Institute, 'The Israeli Democracy Index (2017)' <https://en.idi.org.il/publications/6688> accessed 25 March 2023.

[34] ibid.

This paradox reflects broader cultural and social factors specific to the Israeli context. As one study notes, "The collectivist nature of Israeli society encourages information sharing as part of community identity, even at the expense of privacy [35]".This cultural tendency, combined with the heightened security concerns that characterize Israeli society, creates a distinctive context for privacy perceptions that differs from other democratic institutions.

4.3 The Enforcement Gap.

4.3.1 Case Study: The Enforcement Gap as Epistemic Crisis.

The stark empirical data concerning privacy enforcement reveal more than mere procedural failures; they illuminate a fundamental epistemic crisis in privacy law. The Future of Privacy Forum's study, which found that only 12% of civil claims under the Privacy Protection Law were successful, represents not simply an enforcement gap but a systemic failure to recognize privacy harms as legally cognizable injuries. This crisis is particularly evident in cases involving database violations, which are virtually absent from civil litigation despite their central role in digital surveillance. This absence reflects the law's conceptual blindness to forms of privacy harm that do not manifest as immediate, individualized, and tangible injuries. When privacy violations occur through data processing, which is often invisible, cumulative, and delayed in its effects, the traditional harm-based legal framework fails to provide meaningful recognition or redress.

The data showing that privacy-related class actions represent only 4.5% of all class actions in Israel further demonstrates this epistemic failure. Class actions theoretically provide a mechanism for addressing collective harms that might be individually diffuse. Yet their underutilization in privacy contexts suggests that even collective legal mechanisms remain trapped within an individualistic harm paradigm that cannot adequately conceptualize privacy violations as structural or societal harms. This case study illustrates the broader theoretical problem identified earlier: the legal system continues to rely on observable, measurable "harms" as triggers for legal intervention, even as the most serious surveillance harms have become normalized, invisible, or deferred. The enforcement gap is thus not merely a practical problem of insufficient litigation or legal barriers, but a manifestation of the fundamental inadequacy of harm-based privacy frameworks in the surveillance age.

5. Developing New Legal Tests for "Reasonable Harm".

The preceding analysis demonstrates the inadequacy of current approaches to defining "reasonable harm" to privacy in digital surveillance contexts. This section proposes new legal tests to provide more nuanced, context-sensitive approaches to evaluating privacy violations in the digital age.

[35] 'Privacy in New Media in Israel: How Social Networks are Helping to Shape the Perception of Privacy in Israeli Society' (2018) 17 Journal of Media Studies 203, 220.

5.1 The Chilling Effect Test.

A crucial dimension of privacy harm that is often overlooked in traditional legal frameworks is the "chilling effect" that surveillance can have on protected activities and democratic participation. A new legal test for reasonable harm should explicitly incorporate assessment of these chilling effects, recognizing that privacy violations can cause harm beyond direct informational disclosures.

Under this proposed test, courts would evaluate:

1. Whether the surveillance measure in question has a demonstrable or likely effect on lawful behavior, including political expression, association, or other constitutionally protected activities.
2. The extent to which individuals are aware of the surveillance measure and might reasonably modify their behavior in response.
3. Whether particular groups or communities are disproportionately affected by potential chilling effects, especially those that have historically been subject to heightened monitoring.

5.2 The Contextual Integrity Framework.

Drawing on Nissenbaum's theory of contextual integrity, this proposed test would assess privacy violations by whether they transgress contextual informational norms rather than by absolute public-private distinctions. This approach is particularly well-suited to addressing privacy in networked digital environments.

Under this test, courts would evaluate:

1. The context in which information was shared or collected, including the relationships between parties and the purpose of sharing;
2. Whether the subsequent use, processing, or dissemination of the information violated reasonable expectations within that context;
3. Whether the information flow transgressed established norms for similar contexts in ways that individuals could not reasonably anticipate.

This test finds support in emerging Israeli case law, particularly in decisions such as Ploni v. The Regional Rabbinical Court in Netanya (HCJ 6650/04) and Jarais v. State of Israel (Criminal Appeal 2126/05), which have begun to move away from strict spatial definitions of privacy toward more contextual understandings.[36] It would provide a more flexible framework for addressing privacy violations in digital contexts where traditional boundaries between public and private spaces are increasingly blurred.

5.3 The Proportionality Requirement.

Drawing on Israel's constitutional proportionality test, this proposed approach would incorporate a structured proportionality analysis tailored explicitly to surveillance contexts. While proportionality principles are already applied in some privacy cases, a more structured framework would provide greater consistency and clarity.

Under this test, courts would systematically evaluate:

[36] HCJ 6650/04 *Ploni v The Regional Rabbinical Court in Netanya* (unpublished).

1. Whether the surveillance measure serves a legitimate aim;
2. Whether the measure is suitable for achieving that aim;
3. Whether the measure is necessary, in the sense that no less privacy-invasive alternative would achieve the same aim;
4. Whether the measure is proportionate in the narrow sense, meaning that the importance of the aim justifies the extent of the privacy infringement.

This structured approach would require authorities to demonstrate not only that surveillance measures serve legitimate security or law enforcement purposes, but also that they represent the least invasive means of achieving those purposes. It would provide a more rigorous framework for assessing the reasonableness of privacy infringements in security contexts.

5.4 The Independent Oversight Mechanisms.

A final proposed test focuses not on the nature of the surveillance itself but on the procedural safeguards surrounding it. This test recognizes that the reasonableness of privacy infringements depends not only on their substantive characteristics but also on the oversight mechanisms that prevent abuse.

Under this test, courts would evaluate:

1. Whether prior independent authorization was required and obtained for the surveillance measure.
2. Whether ongoing independent oversight exists to monitor implementation and prevent scope creep.
3. Whether affected individuals have meaningful opportunities for ex post review and redress.

This test addresses concerns raised by empirical evidence showing that nearly 100% of surveillance requests are approved in Israel, with 99.3% of wiretap requests approved in 2021. It recognizes that effective oversight[37] is essential for ensuring that surveillance remains within reasonable bounds and does not result in disproportionate privacy violations.

6. Conclusion: Reimagining Privacy Protections in an Era of Pervasive Surveillance.

This article has examined the complex challenge of defining "reasonable harm" to privacy in the context of digital surveillance, with a particular focus on the Israeli legal framework. Through analysis of theoretical approaches, empirical evidence, and legal developments, it has identified significant gaps between formal legal definitions and public perceptions of privacy violations. These gaps complicate efforts to establish coherent standards for evaluating when surveillance activities cross the threshold from legitimate security measures to disproportionate intrusions on privacy.

The analysis highlights several key findings with broader implications for privacy protection in democratic societies. First, traditional spatial conceptions

[37] A Viner and H Tamam Ben-Avraham, 'Intrusion and Search Technologies in Smart Devices and Digital Assets Employed by Law Enforcement Authorities in Israel' (January 2023) 35.

of privacy centered on distinctions between "public" and "private" spaces are increasingly inadequate in digital contexts where information flows transcend physical boundaries. Israeli courts have begun to recognize this inadequacy; however, statutory frameworks have not yet fully incorporated this evolving understanding.

Second, empirical research reveals significant disparities between expressed privacy concerns and actual privacy-protective behaviors among Israeli citizens, a manifestation of the "privacy paradox" observed in other contexts. These disparities are shaped by cultural, social, and historical factors specific to the Israeli context, including the collectivist nature of Israeli society and heightened security concerns. They complicate efforts to establish objective standards for "reasonable" privacy expectations and highlight the need for context-sensitive approaches.

Third, the current legal framework governing surveillance in Israel contains significant gaps and inconsistencies. The dual-track system for authorizing surveillance, with weaker protections for security-related monitoring compared to law enforcement activities, creates disparities in oversight. High approval rates for surveillance requests raise questions about the effectiveness of judicial authorization as a safeguard against disproportionate privacy violations.

Based on these findings, the article has proposed new legal tests for evaluating "reasonable harm" to privacy in surveillance contexts. These tests incorporate considerations of chilling effects on protected activities, contextual informational norms, structured proportionality analysis, and procedural safeguards. Together, they provide a more comprehensive framework for assessing privacy violations that accounts for both direct and indirect effects, individual and societal impacts, and substantive and procedural dimensions of privacy protection.

The path forward requires not merely incremental legal reforms but a paradigmatic shift in how we conceptualize privacy and its relationship to surveillance in democratic societies. This article argues that the legal system must abandon harm-based thresholds altogether in surveillance law. The traditional requirement to demonstrate "reasonable harm" as a prerequisite for legal intervention has proven fundamentally inadequate in addressing the structural, cumulative, and often invisible nature of privacy violations in the digital surveillance era. Instead, the article proposes a radical inversion of the current framework: a presumption of harm should attach to all unconsented data collection by state actors. This presumption would shift the burden of justification to the surveillance authority, requiring it to demonstrate not merely that the harm is "reasonable", but that the surveillance activity serves a compelling interest that cannot be achieved through less intrusive means. Such a shift would recognize that in an era of pervasive surveillance capabilities, privacy protection requires proactive safeguards rather than reactive remedies for demonstrable harms. Moreover, the legal system must reconceptualize privacy not merely as an individual right but as a structural precondition for democratic participation. The current individualistic focus of privacy law fails to account for the collective dimensions of surveillance, including how it shapes

public discourse, chills political expression, and reinforces existing power asymmetries.

By recognizing privacy as a public good essential to democratic functioning, rather than merely a personal preference subject to individual trade-offs, the legal system can develop more robust protections against surveillance excesses. The Israeli experience with its distinctive combination of security challenges, democratic values, and technological innovation offers valuable insights for this necessary reconceptualization of privacy protection. By confronting the fundamental contradictions in its legal framework and developing new approaches that move beyond harm-based paradigms, Israel can pioneer a more effective model for protecting privacy in the surveillance age. Such innovation is urgently needed not only in Israel but in democracies worldwide grappling with similar tensions between security imperatives and fundamental rights.