International Journal of Innovative Information Systems & Technology Research 14(3):413-429, July-Sept, 2026

© SEAHI PUBLICATIONS, 2026 www.seahipublications.org **ISSN: 2467-8562**

DOI:10.5281/zenodo.22955229

Software Piracy And Its Implications: Determinants, Evidence, Risks, And Policy Responses

Timinipre Amabie*; Laeticia Nneka Onyejegbu; Barilee Baridam

Department of Computer Science,
Faculty of Computing,
University of Port Harcourt, Rivers State, Nigeria.
***Corresponding Author: amabietimi@gmail.com**

ABSTRACT

Software piracy involves unauthorized copying, distribution or other exploitation of protected software, while licence noncompliance also includes contractual uses that require separate legal assessment. This narrative review examines behavioral, economic, organizational, cybersecurity and legal evidence, with particular attention to Nigeria. Across the reviewed studies, attitudes, peer norms, moral beliefs, affordability, access and institutional conditions are associated with piracy, although the evidence varies by population and outcome. Historical BSA/IDC estimates place unlicensed personal-computer software installations at 37% worldwide and 80% in Nigeria in 2017; these figures do not measure current prevalence or all software-delivery models. A 2024 malware study examined 750 pirated-software samples with seven antivirus engines and reported average detection rates of 34% for adware and 35% for trojans, without establishing the prevalence of malware in all unauthorized software. A 2025 survey of 338 United States undergraduate business students further identified associations between neutralization, religiosity and piracy intention. Computer programs receive copyright protection as literary works under TRIPS and Nigeria's Copyright Act 2022, which commenced in 2023, while the Cybercrimes Act 2015 and its 2024 amendment address separate offences. The synthesis supports combining lawful access, licence education, procurement controls, software inventories and proportionate enforcement, with direct evaluation of their effects in the intended setting. Research priorities include contemporary Nigerian prevalence data, clearer distinctions between intention and behavior, and reproducible assessment of security and economic consequences.

Keywords: software piracy; copyright; software licensing; digital piracy; cybersecurity; Nigeria; intellectual property

1. INTRODUCTION

Software is an information good: once developed, an additional digital copy can be reproduced and transmitted at very low marginal cost while retaining essentially the same functional content. That economic property creates legitimate opportunities for rapid diffusion, cloud delivery and open collaboration, but it also lowers the physical barriers to unauthorized copying. Early economic models therefore treated piracy as a strategic issue involving pricing, protection, network effects and diffusion rather than as a simple one-for-one conversion of every unauthorized copy into a lost sale (Conner & Rumelt, 1991; Givon et al., 1995; Shy & Thisse, 1999; Takeyama, 1994, 1997). Later work similarly

showed that the welfare, diffusion and innovation effects of piracy can vary by market structure, installed-base effects, consumer heterogeneity and firm response (Chen & Png, 2003; Prasad & Mahajan, 2003; Sundararajan, 2004). At the behavioral level, software piracy has been studied as an ethical decision, an infringement decision and a form of technology-enabled deviance. Empirical studies repeatedly show that attitudes, peer beliefs, perceived consequences, moral obligation, habit, facilitating conditions and perceived behavioral control matter, although their effect sizes and relative importance vary across samples and contexts (Al-Jabri & Abdul-Gader, 1997; Al-Rafee & Cronan, 2006; Cronan & Al-Rafee, 2008; Limayem et al., 2004; Peace et al., 2003). This multidimensional evidence cautions against explaining piracy only by the price of legal software or only by weak law enforcement.

Software licensing and the legal basis of liability require careful distinction. Software distributed under an open-source licence remains subject to copyright, even when the licence permits extensive copying and modification. The Apache License 2.0 and GNU General Public License version 3 illustrate different conditions governing redistribution and derivative works (Apache Software Foundation, 2004; Free Software Foundation, 2007). Nigerian copyright and cybercrime law also operate through distinct statutes: the Copyright Act 2022 protects computer programs, while the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended in 2024, addresses conduct within its separate scope (Federal Republic of Nigeria, 2015, 2023, 2024). This article examines the forms, determinants, scale and implications of software piracy, together with responses relevant to Nigeria. It distinguishes historical industry estimates from contemporary prevalence, contractual noncompliance from copyright infringement, and statistical association from causal evidence.

This article uses a narrative-review approach to synthesize scholarship and primary institutional materials concerning software piracy. The discussion covers definitions, determinants, historical prevalence, cybersecurity, economic effects, legal provisions and intervention options. Foundational studies are retained where they establish theories or measures used in subsequent research. Evidence is considered at the individual, organizational, national and market levels, with attention to whether each source offers a theoretical mechanism, an empirical association or a design intended to support causal inference. Industry estimates are attributed to their producing organization and interpreted within their stated scope. The review does not pool effect sizes or claim exhaustive coverage of the literature. Differences in samples, outcome definitions and publication periods limit direct comparison across studies.

2. Conceptual, Licensing, and Legal Foundations

2.1 Defining software piracy and licence noncompliance

Software piracy refers here to unauthorized reproduction, distribution or other exploitation of protected software that infringes copyright. Licence noncompliance is a related but broader category, because exceeding a contractual restriction does not necessarily establish copyright infringement or a criminal offence. Research therefore needs to distinguish the conduct observed from the legal characterization assigned to it. Workplace and end-user studies have examined unauthorized copying and softlifting, including installation beyond permitted users or devices (Cheng et al., 1997; Moores & Dhillon, 2000; Peace et al., 2003; Simpson et al., 1994). A software purchaser commonly receives specified permissions without acquiring the underlying copyright. Article 10 of TRIPS requires protection of computer programs in source and object code as literary works, while sections 9 and 108 of Nigeria's Copyright Act 2022 specify relevant exclusive rights and include computer programs within literary works (Federal Republic of Nigeria, 2023; World Trade Organization, 1994). The applicable licence, statutory exceptions and facts of the transaction must therefore be considered together.

Open-source licensing provides lawful permissions within the copyright system. The Apache License 2.0 permits reproduction and redistribution subject to conditions that include supplying the licence and retaining relevant notices (Apache Software Foundation, 2004). The GNU General Public License version 3 applies different conditions to conveying covered modified works and object code, including

requirements concerning corresponding source code (Free Software Foundation, 2007). These examples show why a general label such as open source does not establish the obligations attached to a particular component. Freeware and shareware are commonly used distribution labels, but neither label alone establishes a right to modify or redistribute a program. Researchers and procurement officers should record the actual licence, its version and the intended use. Price, source-code availability and copyright permissions should be assessed separately.

2.2 Theoretical explanations

No single theory explains software piracy across all contexts. The theory of planned behavior proposes that intention is shaped by attitudes, subjective norms and perceived behavioral control (Ajzen, 1991). Software-piracy studies have repeatedly adapted this logic, often adding moral obligation, past behavior or ethical judgment (Al-Rafee & Cronan, 2006; Cronan & Al-Rafee, 2008; Peace et al., 2003). Social-learning and peer-belief findings further show that perceived behavior and approval by relevant others can normalize infringement (Al-Jabri & Abdul-Gader, 1997; Hinduja, 2001, 2003; Limayem et al., 2004). Intention is an expressed willingness to act, whereas behavior concerns the action itself, so evidence about one should not automatically be interpreted as evidence about the other.

Deterrence perspectives derive from the idea that misconduct becomes less attractive as the perceived probability and cost of sanction increase (Becker, 1968). Software-piracy studies also examine informal controls, moral beliefs and peer effects alongside formal sanctions (Siponen et al., 2012). Neutralization theory explains how individuals temporarily rationalize behavior that conflicts with general norms; software-piracy research has found support for particular rationalizations, while also showing that neutralization is not uniformly strong across samples (Hinduja, 2007; Siponen et al., 2012; Sykes & Matza, 1957). Moral disengagement and ethical self-efficacy similarly help explain why individuals may distance themselves from perceived harm or feel more capable of resisting unethical computer behavior (Bandura, 1999; Kuo & Hsu, 2001). These theories identify plausible mechanisms, but the importance of each mechanism requires empirical assessment in the population under study.

Economic models add market-level mechanisms. When legal prices are high relative to income, lawful distribution is limited, or unauthorized copies are easy to obtain, the private cost-benefit calculation changes. At the same time, network effects mean that some unauthorized use can expand an installed base, complicating simple estimates of displaced sales; firms may respond through pricing, product differentiation, subscriptions, complementary services, private technical protection or innovation (Chen & Png, 2003; Conner & Rumelt, 1991; Gopal & Sanders, 1998; Jaisingh, 2009; Peitz & Waelbroeck, 2006). Recent firm-level evidence also shows that piracy shocks can induce heterogeneous innovation responses rather than a uniform reduction in innovation, reinforcing the need to avoid overstated causal claims (Bradley & Kolev, 2023). The resulting predictions concern specified market conditions and should not be interpreted as a general estimate of the effects of infringement.

Figure 1 organizes the proposed relationships between software-piracy determinants, individual appraisals, behavior and consequences. Economic conditions, social norms and legal or organizational arrangements provide the context in which users assess their options. Attitudes, perceived control and expected consequences can then influence intention and action. Experiences following use may alter later risk perceptions and organizational decisions. The arrows represent relationships synthesized from the cited theories and studies, rather than coefficients estimated in a single validated model. The framework provides a basis for comparing studies while retaining their differences in population, measurement and setting.

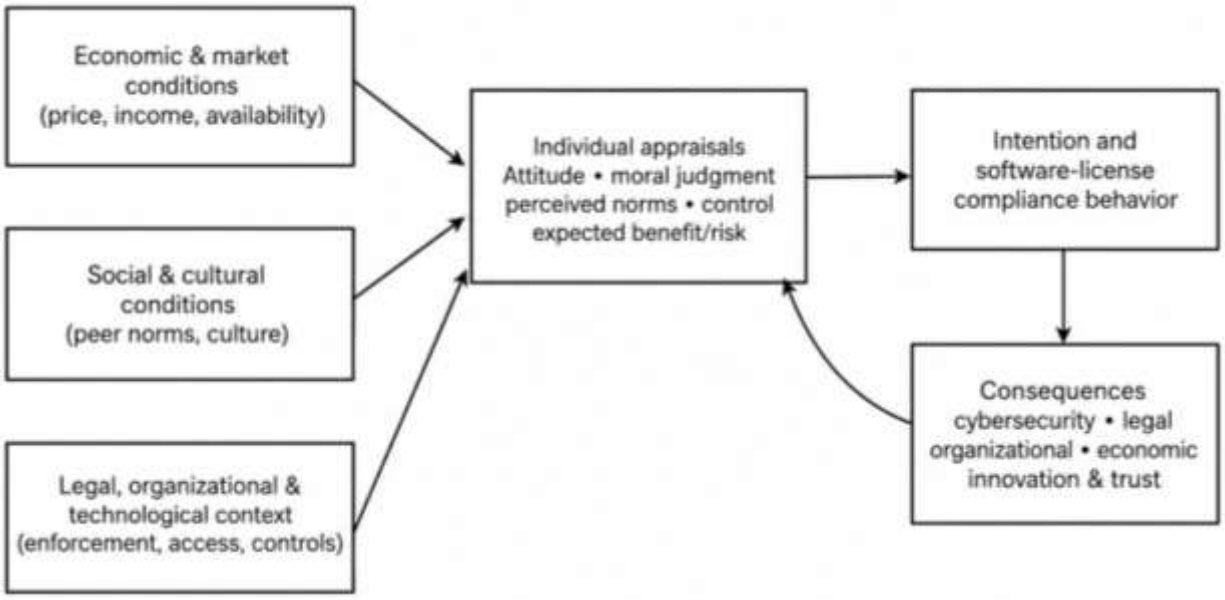

Figure 1. Integrated framework for software-piracy determinants, behavior, and consequences

Note. Author synthesis based on Ajzen (1991), Al-Rafee and Cronan (2006), Becker (1968), Gopal and Sanders (1998), Limayem et al. (2004), Peace et al. (2003), and Siponen et al. (2012).

3. Forms of Software Piracy and Licence Noncompliance

The terminology used in anti-piracy literature developed around physical media and perpetual desktop licences. Some labels remain useful, but the underlying principle is more durable: a use becomes infringing or noncompliant when it exceeds the permissions granted by law or licence. Table 1 shows the traditional typology without implying that every licensing dispute is criminal or that every unauthorized copy has the same legal consequences. It also shows why older categories should not be treated as mutually exclusive. A single transaction may combine unauthorized distribution, counterfeiting and over-installation. Conversely, a licence breach does not automatically establish every element of a criminal copyright offence. For research and compliance purposes, studies should state exactly what behavior is measured rather than using the word 'piracy' as an undifferentiated label.

Table 1. Common forms of software piracy and licence noncompliance

Form	Core description	Typical actor/setting	Principal issue	References
Softlifting / over-installation	Installing or sharing a licensed copy beyond the number of authorized users or devices.	Individuals; workplaces	Licence noncompliance and copyright infringement depending on facts.	Simpson et al. (1994); Peace et al. (2003)
Client-server or concurrent-use overuse	Making software available to more simultaneous users than the purchased entitlement permits.	Organizations	Asset-management and licence-compliance risk.	Peace et al. (2003); Moores & Dhillon (2000)
Hard-disk loading	Supplying computers with unauthorized commercial software pre-installed to increase sale value.	Hardware resellers	Distribution and reproduction without authorization.	BSA | The Software Alliance (2018); Moores & Dhillon (2000)

Form	Core description	Typical actor/setting	Principal issue	References
Counterfeiting	Producing or selling copies presented as genuine commercial software.	Distributors; vendors	Copyright, trademark, fraud and cybersecurity concerns may overlap.	BSA | The Software Alliance (2018); Iqbal et al. (2024)
Unauthorized online distribution	Making protected software available through online channels without the right holder's authorization.	Uploaders; distributors	Large-scale reproduction/distribution; platform and jurisdiction issues.	Hinduja (2003, 2007); Peitz & Waelbroeck (2006)
Academic or restricted-licence misuse	Using software supplied under educational, noncommercial or other restricted terms for an unauthorized purpose.	Students; institutions; businesses	Breach of licence terms; possible copyright infringement.	Gan & Koh (2006); Mishra et al. (2006)
Subscription/account overuse	Using seats, credentials or access rights beyond contractual entitlement.	Individuals; organizations	Primarily contractual/licensing issue; facts determine copyright implications.	BSA | The Software Alliance (2018); author synthesis of entitlement-based licensing
Circumvention-linked infringement	Using unauthorized modifications to defeat access or licence controls in order to use protected software without permission.	Technically skilled users; distributors	May engage copyright, anti-circumvention and cybercrime rules depending on jurisdiction.	Djekic & Loebbecke (2007); Federal Republic of Nigeria (2023)

4. Determinants of Software Piracy

4.1 Psychological, ethical, and behavioral factors

Attitude toward piracy is a recurring individual-level predictor of intention. In their study, Al-Rafee and Cronan (2006) reported associations of digital-piracy attitudes with outcome beliefs, affective beliefs, subjective norms and other individual characteristics. Cronan and Al-Rafee (2008) subsequently showed that a model incorporating attitude, perceived behavioral control, past behavior and moral obligation explained a substantial share of variance in intention. Peace et al. (2003) likewise found support for an integrated workplace model in which attitude, subjective norms and perceived behavioral control influenced software-piracy intention. Because these outcomes concern reported attitudes or intentions, they do not by themselves demonstrate a reduction in unauthorized installations following an intervention.

Ethical judgment is not reducible to legal knowledge. Early studies examined ethical perceptions, situational equity and characteristics of software users (Glass & Wood, 1996; Sims et al., 1996; Wagner & Sanders, 2001). Logsdon et al. (1994) found only limited support for a relationship between moral judgment and unauthorized copying, emphasizing the need to distinguish general moral reasoning from the perceived seriousness of software piracy. Kuo and Hsu (2001) developed an ethical computer self-efficacy construct around resisting softlifting, illustrating that confidence in one's ability to refrain from or discourage piracy is distinct from simply knowing that the act is prohibited. Douglas et al. (2007) further found that equity perceptions can operate as a deterrent, suggesting that users' judgments about fairness influence compliance. Measures of fairness, moral judgment and ethical confidence should therefore be reported separately instead of being combined under an unspecified measure of awareness.

Neutralization describes rationalizations used to justify conduct that would otherwise conflict with a person's accepted norms. Hinduja (2007) found a weak overall relationship between neutralization and reported online software-piracy experience in a United States university sample. Siponen et al. (2012), studying 183 respondents, identified associations between particular neutralizations, shame, moral beliefs

and piracy intention. Ingram and Hinduja (2008) examined music piracy, providing related evidence whose application to software requires separate testing. Lau (2003) examined software-piracy decisions and contributes software-specific evidence to this broader discussion. The contrast between studies shows why past behavior, current intention and different types of digital content should be distinguished. It also indicates that legal knowledge alone is an incomplete measure of the reasoning associated with unauthorized use.

Sikolia et al. (2025) provide more recent evidence from 338 undergraduate business students in the United States. Their structural equation model identified condemning the condemners, appealing to higher loyalties and the ledger metaphor as predictors of software-piracy intention. The ledger metaphor describes the justification of misconduct by reference to an individual's other good actions. Intrinsic religiosity was negatively associated with intention, whereas extrinsic religiosity was positively associated with it. These findings concern self-reported intention in a student sample and do not establish either national prevalence or a causal effect of religious participation. They support distinguishing specific rationalizations and dimensions of religiosity when designing further software-piracy research.

4.2 Social, cultural, and educational factors

Peer beliefs and social norms repeatedly predict piracy intention. Al-Jabri and Abdul-Gader (1997), using a scenario study in Saudi Arabia, found significant effects of individual and peer beliefs on intention to observe or infringe software copyright. Limayem et al. (2004) found social factors and beliefs about consequences to affect piracy intention in a longitudinal design, while habit and facilitating conditions were related to actual behavior. Tang and Farn (2005) examined interpersonal influence through a laboratory experiment involving 54 participants and a separate survey of 216 college students in Taiwan. These findings justify evaluating interventions aimed at perceived norms, alongside explanations of legal responsibilities.

Cross-national research shows that software piracy also reflects broader institutional and cultural environments. Husted (2000) linked national culture to piracy rates; Marron and Steel (2000) examined why countries differ in intellectual-property protection; and Shadlen et al. (2005) emphasized the political economy of software protection. Moores and Chang (2006) examined ethical recognition, judgment, intention and behavior, while Chang et al. (2017), using cross-national longitudinal data, examined economic, cultural, regulatory and technological determinants. These macro studies cannot establish individual motives, but they help investigate why national piracy rates differ even when software technology is globally available. Africa-focused panel studies likewise report associations between software-piracy indicators and inequality, scientific knowledge production, and inclusive human development, while their aggregate designs warrant caution against individual-level or simple causal interpretation (Asongu, 2014a, 2014b; Asongu & Andrés, 2017).

Education can have competing effects. More education may increase knowledge of copyright and access to legal institutional resources, but it can also increase computer competence and exposure to copying opportunities. Student studies in Singapore and elsewhere show that piracy in educational environments is shaped by attitudes, perceived norms, access and institutional practices rather than academic status alone (Gan & Koh, 2006; Hinduja, 2001, 2003; Sims et al., 1996). Institutional access to licensed software should consequently be measured separately from educational attainment. Evaluations should also distinguish knowledge of licence conditions from the ability to obtain an affordable lawful alternative.

4.3 Economic and market factors

Affordability is an important consideration in the economic literature. Gopal and Sanders (1998) found economic development to be closely related to cross-national piracy, and subsequent studies likewise associated higher income and stronger institutions with lower piracy rates (Husted, 2000; Marron & Steel, 2000; Chang et al., 2017). In lower-income markets, a uniform global price can represent a much larger share of disposable income, increasing the attraction of unauthorized alternatives. However, affordability should not be framed as determinism: peer norms, ethics, availability, enforcement and organizational

policy still matter. Kukla-Gryz et al. (2021) studied customers of an ebook retailer and found an association between perceived overpricing and willingness to obtain books from unauthorized sources. This result supports examining price fairness in software markets, but it does not directly measure the effect of software-price reductions on infringement.

Economic theory also warns against treating the retail price of every unauthorized copy as an automatic loss. Some users of unauthorized copies would not have purchased at the prevailing price, and network effects can change later demand. Givon et al. (1995) explicitly modeled lost sales and diffusion; Takeyama (1994, 1997) showed how unauthorized reproduction can have different welfare implications when network externalities and intertemporal effects are present. This does not make infringement lawful, but it means credible economic-impact studies should estimate displaced sales rather than multiply every unauthorized copy by list price. Estimates should state the assumed purchase counterfactual and distinguish producer revenue from consumer welfare and broader social costs.

Firms can respond through pricing, product differentiation, subscriptions, complementary services and protection strategies. Conner and Rumelt (1991), Shy and Thisse (1999), Chen and Png (2003), Prasad and Mahajan (2003), Sundararajan (2004) and Jaisingh (2009) examine conditions under which pricing, diffusion and protection interact. Excessively burdensome controls can reduce legitimate-user value, while weak controls can increase unauthorized use. Djekic and Loebbecke (2007) examined the effectiveness of technical copy protection among application-software users. The effectiveness of a particular control should therefore be assessed against both unauthorized use and the costs imposed on legitimate users.

4.4 Technological, organizational, and legal factors

Technology affects opportunity. Fast networks, digital distribution and easy replication reduce the effort required to obtain or disseminate unauthorized copies, which helps explain why earlier research linked Internet access and online experience to piracy behavior (Hinduja, 2001, 2003). Technology is not a cause in isolation, however: the same infrastructure supports legal downloads, subscriptions, open-source distribution and remote licence verification. Within organizations, budget constraints, weak asset inventories, decentralized purchasing, employee installation rights and poor licence governance can convert individual behavior into enterprise-wide exposure. Mishra et al. (2006) studied piracy among IT professionals, and Peace et al. (2003) focused on workplace behavior, underscoring that organizational controls and norms matter. Software asset management therefore needs entitlement records, procurement controls, deployment inventories, patching, removal of unsupported software and periodic reconciliation rather than ad hoc enforcement after an audit.

Law influences piracy through both formal rights and perceived enforcement. Statutory protection alone does not ensure compliance; perceived certainty of detection, institutional capacity and judicial effectiveness also affect deterrence. Ginarte and Park (1997) document variation in patent protection, which provides institutional context but is not a measure of software-copyright enforcement. Software-specific studies examine regulatory protection and institutional conditions in relation to national piracy estimates (Chang et al., 2017; Marron & Steel, 2000; Shadlen et al., 2005). These associations are subject to endogeneity because national income, institutional quality and reported piracy rates may influence one another. Individual-level research examines both formal sanctions and informal deterrents (Siponen et al., 2012), while Wolfe et al. (2008) investigate fear of computer viruses in relation to digital-piracy intention.

Table 2 demonstrates the diversity of the evidence base. Much of the behavioral literature relies on student or convenience samples and self-reported intention, whereas country-level studies use aggregate piracy estimates and institutional indicators. These designs answer different questions and should not be merged as though they measure the same construct. Meta-analytic evidence across digital piracy more broadly identifies outcome expectancies, social learning, self-regulation and moral disengagement as recurring predictors, but software-specific policy should still be tested in the target context (Eisend, 2019; Fleming et al., 2017).

Table 2. Selected empirical studies informing software-piracy determinants

References	Setting/design	Sample	Key contribution
Al-Jabri & Abdul-Gader (1997)	Saudi Arabia; scenario survey	Scenario-survey respondents	Peer and individual beliefs significantly affected copyright-compliance intentions.
Hinduja (2007)	U.S. university students	University students	Neutralization had limited overall explanatory power; several other correlates were more salient.
Tang & Farn (2005)	Laboratory experiment and student survey	54 experimental participants; 216 survey respondents	Interpersonal influence affected softlifting intention and behavior.
Gan & Koh (2006)	Tertiary institutions, Singapore	About 500 students and staff	Identified profiles associated with attitudes, convenience, acceptance and ethics in university communities.
Djekic & Loebbecke (2007)	Professional and amateur application-software users	Professional and amateur users	Investigated the effectiveness of technical copy protection among application-software users.
Siponen et al. (2012)	Survey	183	Specific neutralizations, shame and moral beliefs predicted piracy intentions.
Chang et al. (2017)	Cross-national panel	Countries observed longitudinally	Examined economic, cultural, regulatory and technological correlates of national piracy estimates.
Andembubtob et al. (2020)	Nigeria; survey across geopolitical zones	3,270	Reported widespread piracy-related behavior and awareness issues; useful Nigeria-specific evidence but based on self-report.
Iqbal et al. (2024)	Pirated-software samples, Southeast Asia	750 samples reported by study	Examined 750 pirated-software samples using seven antivirus engines; reported average detection rates of 34% for adware and 35% for trojans.
Sikolia et al. (2025)	United States; student survey and structural equation model	338 undergraduate business students	Specific neutralizations and dimensions of religiosity were associated with piracy intention.

Note. Samples and outcomes are described at the level supported by the cited publications. Approximate totals follow the wording of the original study. Intention, self-reported behavior, national estimates and malware detections are distinct outcomes.

5. Scale and Patterns: What the Available Data Can and Cannot Show

The 2018 BSA Global Software Survey reports historical estimates of unlicensed software installed on personal computers. BSA | The Software Alliance (2018), working with IDC, covered more than 110 national and regional economies. Its installation rate concerns PC software and should not be interpreted as a measure of every form of software use. In particular, a PC-installation indicator does not directly measure server-software use, mobile applications or cloud-account entitlement. The estimates therefore require an explicit reference year and a clear statement of the population measured.

For 2017, BSA estimated a worldwide unlicensed PC-software installation rate of 37% and a commercial value of US$46.302 billion. For Nigeria, the reported rate was 80% with a commercial value of US$123 million. The Middle East and Africa regional estimate was 56%. Kenya was reported at 74%, while South

Africa was 32%. These figures are useful for historical comparison but are produced by an industry association and depend on estimation assumptions; independent contemporary measurement is therefore a major research need (BSA | The Software Alliance, 2018).

Table 3 presents the historical installation rates and commercial values, while Figure 2 compares the worldwide and Nigerian rate series. The worldwide estimate changed from 42% in 2011 to 37% in 2017, a decline of five percentage points. Nigeria's corresponding estimate changed from 82% to 80%, a decline of two percentage points. The values describe four reported observations rather than a continuously measured annual series. Commercial value is the estimated value assigned to unlicensed software and should not be treated as observed revenue that producers would necessarily have received. Contemporary measurement should cover the relevant delivery and licensing models instead of extrapolating these historical rates (BSA | The Software Alliance, 2018).

Table 3. BSA/IDC historical estimates of unlicensed PC software, 2011–2017

Geography	Year	Unlicensed rate (%)	Commercial value (US$ billions)
Worldwide	2011	42	63.456
Worldwide	2013	43	62.709
Worldwide	2015	39	52.242
Worldwide	2017	37	46.302
Nigeria	2011	82	0.251
Nigeria	2013	81	0.287
Nigeria	2015	80	0.232
Nigeria	2017	80	0.123
Middle East & Africa	2017	56	3.077
Kenya	2017	74	0.099
South Africa	2017	32	0.241

Note. Source: BSA | The Software Alliance (2018, pp. 10–11). Commercial values are expressed in US$ billions; the source reports US$ millions. Installation rates concern personal-computer software. The observations are historical estimates and are not measures of current prevalence or directly observed lost sales.

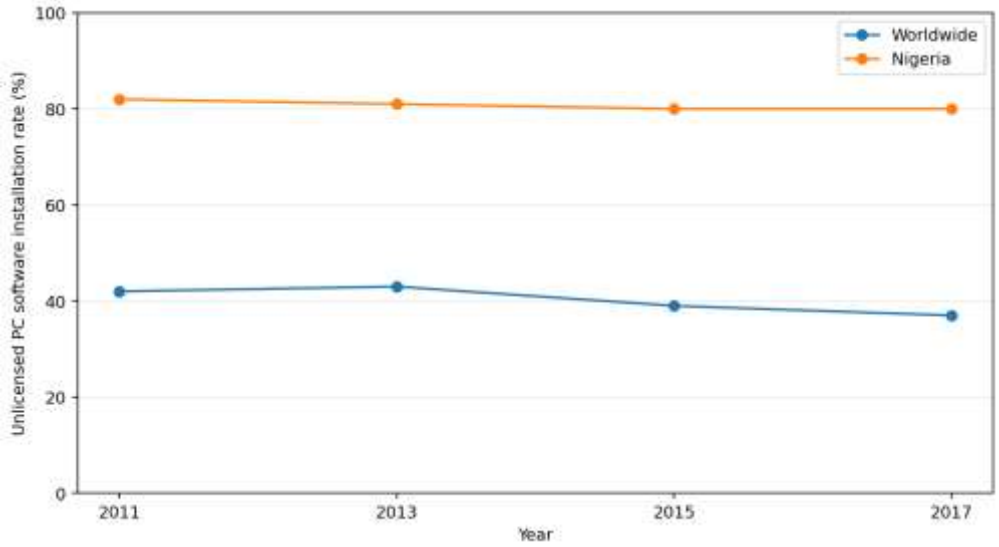

Figure 2. Worldwide and Nigeria unlicensed PC-software installation rates, 2011–2017

Note. Source: BSA | The Software Alliance (2018). The series reflects estimated unlicensed software installed on PCs. It should not be extrapolated mechanically beyond 2017.

6. Implications of Software Piracy

6.1 Cybersecurity and operational risk

Software obtained through unauthorized distribution channels can contain malicious code, although the occurrence of infringement does not itself establish malware infection. Iqbal et al. (2024) examined 750 pirated-software samples drawn from physical media and online sources, using seven antivirus engines. The reported average detection rates were 34% for adware and 35% for trojans. The study also identified changes affecting firewall and user-account-control settings after installation. These findings concern the sampled material and the detection methods employed. The two malware percentages should not be added to infer an overall infection rate because the reported categories and engine averages do not establish mutually exclusive proportions. The results identify a security concern without estimating a universal risk for all unauthorized software or for Nigeria.

Software governance connects licence management with cybersecurity, although the two objectives require different evidence. An inventory can identify deployed applications, versions and responsible owners, while entitlement records establish whether the organization has permission for those deployments. The NIST Cybersecurity Framework 2.0 includes maintaining inventories of software, systems and services and managing software throughout its life cycle (Pascoe et al., 2024). These outcomes provide a basis for identifying unsupported applications and coordinating maintenance with procurement. BSA | The Software Alliance (2018) also discusses security and licence management, but its industry-sponsored estimates do not establish the causal effect of each control. A valid licence alone does not guarantee security, and a malware detection alone does not determine licence status.

6.2 Legal, financial, and reputational implications

Unauthorized reproduction or distribution may engage civil remedies or criminal provisions when their respective statutory requirements are met. Nigeria's Copyright Act 2022 commenced on 17 March 2023 and was published as Act No. 8 in the 2023 Gazette. Sections 9 and 108 establish relevant rights and include computer programs within literary works, while sections 50–52 concern technological protection measures and rights-management information (Federal Republic of Nigeria, 2023). These provisions must

be read with their exceptions, including the conditions specified for certain interoperability activities. Separate conduct such as unauthorized access may fall within the Cybercrimes Act 2015, as amended in 2024 (Federal Republic of Nigeria, 2015, 2024). Liability therefore depends on the conduct proved and the applicable statutory elements, rather than the general label of piracy.

For organizations, the financial consequences extend beyond damages or licence true-up costs. Investigations can consume staff time, disrupt operations, create procurement costs and expose weak governance. Reputational consequences may arise where customers, partners or regulators interpret unlicensed software as evidence of poor controls. These operational and reputational outcomes are context-dependent. Because legal consequences depend on the proven conduct, governing licence, remedies sought and applicable statutory provisions, neither a universal fine nor automatic imprisonment can be inferred for all forms of software licence noncompliance (BSA | The Software Alliance, 2018; Federal Republic of Nigeria, 2015, 2023, 2024).

6.3 Economic, innovation, and welfare implications

Piracy can reduce revenue available to software producers when unauthorized use displaces purchases, and this can weaken expected returns to development. Cross-national and industry studies have therefore treated piracy as an innovation and investment issue (Gopal & Sanders, 1998; Shadlen et al., 2005). Yet the magnitude of lost sales is empirically difficult to infer because not every unauthorized user would purchase at the observed price. Givon et al. (1995) explicitly separated diffusion and lost-sales effects, while the theoretical literature identifies network externalities and indirect appropriation as reasons why welfare outcomes can be non-linear (Peitz & Waelbroeck, 2006; Takeyama, 1994, 1997). Economic analysis should therefore specify whose revenue or welfare is measured and over what period.

Firm responses to piracy vary with market position and the opportunities available to them. Jaisingh (2009) develops a theoretical account of piracy and innovation incentives. Bradley and Kolev (2023) use a quasi-experimental design based on a 2001 technological shock that increased exposure to software piracy. They report subsequent increases in research and development spending and intellectual-property filings among large incumbent software firms. The findings concern a particular shock and group of firms, rather than every producer or software market. They indicate that innovation may form part of a competitive response and do not establish that infringement improves overall welfare. Policy analysis should distinguish these measured responses from legal rights and from unmeasured effects on smaller firms or new entrants.

7. Responses to Software Piracy and Licence Noncompliance

Table 4 links proposed responses to the mechanisms and risks discussed in the literature. Affordable lawful access addresses the options available to users, while education addresses understanding, attitudes and rationalization. Organizational controls establish responsibility for procurement, installation and licence records. Technical measures and enforcement address different aspects of unauthorized access and infringement. These components should be selected according to the conduct, population and institutional capacity concerned. Their effectiveness should be evaluated with defined outcomes rather than inferred solely from the plausibility of the proposed mechanism.

Table 4. Proposed responses to software piracy and licence noncompliance

Intervention	Primary mechanism	References	Implementation caution
Affordable lawful access and localized pricing	Reduces the private economic benefit of unauthorized alternatives.	Gopal & Sanders (1998); Chen & Png (2003); Sundararajan (2004)	Must preserve sustainable revenue and avoid arbitrary geographic exclusion.
Education and norm correction	Targets attitudes, moral judgment, neutralization and perceived peer approval.	Al-Jabri & Abdul-Gader (1997); Al-Rafee & Cronan (2006); Siponen et al. (2012)	Evaluate whether explanations of licence terms and rationalizations change actual compliance.

Intervention	Primary mechanism	References	Implementation caution
Software asset management	Improves entitlement records, deployment control and reconciliation.	Peace et al. (2003); Mishra et al. (2006); BSA | The Software Alliance (2018)	Requires central ownership, procurement records and periodic inventory.
Technical protection and authenticated distribution	Raises effort and reduces exposure to tampered copies.	Djekic & Loebbecke (2007); Iqbal et al. (2024)	Protection should not impose excessive burdens on legitimate users.
Credible and proportionate enforcement	Raises expected cost where violations are deliberate and material.	Becker (1968); Chang et al. (2017); Federal Republic of Nigeria (2023)	Assess detection capacity, due process and proportionality in the intended jurisdiction.
Open-source and appropriately licensed alternatives	Provides lawful substitutes where budgets or teaching needs constrain proprietary licensing.	Apache Software Foundation (2004); Free Software Foundation (2007)	Organizations must still comply with open-source licence obligations.
Organizational least-privilege installation and patch governance	Supports control of software inventories, access and maintenance.	Pascoe et al. (2024); Iqbal et al. (2024)	Must be paired with approved-software workflows so users can work effectively.

Note. The table synthesizes theoretical mechanisms, observational evidence, legal authorities and organizational guidance. Inclusion does not imply that an intervention has been shown to reduce piracy in a randomized trial. Effects require evaluation in the intended setting.

Behavioral evidence suggests that awareness campaigns should move beyond repeating that piracy is illegal. Users may already know the rule but discount harm, believe peers approve, perceive little chance of detection, or see the legal option as inaccessible. Communication can therefore clarify licence rights, correct exaggerated beliefs about peer behavior, explain concrete organizational and cybersecurity consequences, and make lawful alternatives easy to obtain (Al-Rafee & Cronan, 2006; Douglas et al., 2007; Siponen et al., 2012). Such campaigns should specify the behavior they seek to change and the lawful route through which users can meet their needs. Evaluation should measure knowledge and reported intentions separately from subsequent installations or other compliance outcomes.

Organizations should establish a continuing process for licence compliance. Procurement records should identify the product, permitted users or devices, term of use and responsible owner. Deployment inventories should then be reconciled with those entitlements, with procedures for renewals, transfers, departures and exceptions (BSA | The Software Alliance, 2018). Cybersecurity assessment should additionally consider version support, vulnerability exposure and the authenticity of distribution channels. The NIST Cybersecurity Framework 2.0 provides relevant outcomes for inventories and life-cycle management, while leaving implementation choices to the organization (Pascoe et al., 2024). Findings from workplace research provide a further reason to examine organizational norms and employee practices alongside formal records (Mishra et al., 2006; Peace et al., 2003).

Technical controls should be proportionate. Economic and empirical work does not support a simplistic assumption that stronger digital restrictions always produce more legitimate sales. Restrictions can impose usability costs on paying customers, while determined infringers may circumvent them (Djekic & Loebbecke, 2007; Peitz & Waelbroeck, 2006). Technical protection is therefore best combined with attractive legal access, account security, authenticated distribution and enforcement targeted at material commercial infringement. Evaluation should include the burden on authorized users, the rate of unauthorized use and the reliability of support and recovery procedures.

8. Nigeria-Focused Legal and Policy Implications

Nigeria's policy response requires coordination between copyright administration, cybercrime enforcement, procurement and education. The legal basis for a case should first be identified from the conduct involved and the rights affected. The Copyright Act 2022, in force from 2023, provides the

principal copyright framework for computer programs and includes measures concerning technological protection and online content (Federal Republic of Nigeria, 2023). The Cybercrimes Act 2015 and its 2024 amendment address offences within their own scope (Federal Republic of Nigeria, 2015, 2024). Article 10 of TRIPS supplies the international requirement to protect computer programs as literary works (World Trade Organization, 1994). Implementation should distinguish deliberate commercial infringement, disputed licence interpretation and administrative noncompliance, while applying the relevant legal provisions to each case.

The historical BSA estimate of 80% unlicensed PC-software installation in Nigeria in 2017 indicates a serious legacy compliance problem, but policy should not rely on that figure as if it measured the present environment (BSA | The Software Alliance, 2018). A contemporary Nigeria study should distinguish personal computers, mobile applications, cloud subscriptions, enterprise SaaS, academic licences and open-source components. It should also separate deliberate infringement from accidental noncompliance caused by weak procurement records or misunderstanding of licence terms. Sampling should cover households, educational institutions, public bodies and businesses rather than assume a single pattern of use. Results should report denominators and uncertainty so that prevalence estimates can be compared over time.

Nigeria-specific surveys provide local evidence that complements cross-national estimates. Andembubtob et al. (2020) reported an online questionnaire sample of 3,270 respondents drawn from Nigeria's six geopolitical zones. The study provides useful local evidence, but its self-reported measures, online recruitment and limited methodological detail constrain representativeness and causal inference. Stronger contemporary designs should combine probability-based user surveys, anonymized organizational software-asset records, legal case data, vendor-independent telemetry where ethically available, and qualitative interviews with universities, SMEs, public institutions and software developers. Participation, data access and the treatment of potentially identifying records should be specified before collection begins.

Affordability and access should be assessed alongside enforcement. Educational institutions and small and medium-sized enterprises can consider institution-wide licences, lawful student editions and suitable open-source alternatives when matching software requirements to available budgets. Economic models provide a basis for examining pricing and access, but do not guarantee the effect of a particular purchasing scheme in Nigeria (Chen & Png, 2003; Gopal & Sanders, 1998). Open-source adoption also requires attention to the conditions of each licence, including distribution and notice requirements (Apache Software Foundation, 2004; Free Software Foundation, 2007). Procurement should record entitlement and software provenance and should provide a documented route for obtaining approved applications. Security assessment should examine the trustworthiness of the distribution channel and the maintenance process, in light of evidence of malware in sampled unauthorized software (Iqbal et al., 2024).

9. Limitations of the Evidence and Priorities for Future Research

The software-piracy literature has four recurring limitations. First, many behavioral studies use students or convenience samples, limiting generalizability to enterprises, public institutions and informal businesses (Gan & Koh, 2006; Hinduja, 2007; Sims et al., 1996). Second, self-reported piracy is vulnerable to social-desirability bias and recall error (Al-Jabri & Abdul-Gader, 1997; Peace et al., 2003; Siponen et al., 2012). Third, country-level studies frequently depend on industry-estimated piracy rates and are subject to omitted-variable and endogeneity problems (BSA | The Software Alliance, 2018; Chang et al., 2017). Fourth, measures developed for packaged PC software do not automatically capture cloud-account overuse, mobile applications or component-level licence obligations.

Future research should prioritize preregistered causal or longitudinal designs, representative African samples, transparent measurement of licence entitlement versus actual deployment, and independent

replication of industry prevalence estimates. Studies should report exact operational definitions: unauthorized installation, account overuse, counterfeit purchase, online distribution and open-source licence noncompliance are not interchangeable outcomes. Cybersecurity research should compare authorized and unauthorized samples using reproducible malware-analysis protocols and documented sampling frames rather than inferring malware risk from anecdotal cases (Iqbal et al., 2024). Meta-analytic and review evidence can help identify robust predictors, but primary studies remain essential for policy. Eisend (2019) synthesized digital-piracy predictors within a social-cognitive framework, and Fleming et al. (2017) combined systematic review, meta-analysis and panel evidence on unlawful file sharing. Their broader findings support attitudes, norms, control, social learning and moral mechanisms, yet software-specific and Nigeria-specific interventions still require direct testing.

10. Conclusion

Software piracy is not adequately explained by a single narrative of high prices, weak morality, weak enforcement or technological ease. The evidence supports an integrated account in which market conditions, social norms, ethical appraisal, perceived control, institutional quality, organizational governance and technology interact. A coordinated response should combine attractive lawful access, licence education, software asset management, proportionate technical controls, cybersecurity hygiene and credible enforcement. Two legal distinctions are central to accurate scholarship and policy design. Open-source and free software remain governed by copyright licences; broad rights to copy or modify exist because a licence grants them, not because copyright is absent. In Nigeria, the Copyright Act 2022 is the principal statute protecting computer programs as literary works, while the Cybercrimes Act 2015, as amended in 2024, addresses separate computer and cyber offences where its elements are met.

Acknowledgements

This study forms part of the lead author's PhD thesis at the University of Port Harcourt, Nigeria, under the supervision and scholarly guidance of the other authors.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Al-Jabri, I. M., & Abdul-Gader, A. H. (1997). Software copyright infringements: An exploratory study of the effects of individual and peer beliefs. *Omega, 25*(3), 335–344. https://doi.org/10.1016/S0305-0483(96)00053-9

Al-Rafee, S., & Cronan, T. P. (2006). Digital piracy: Factors that influence attitude toward behavior. *Journal of Business Ethics, 63*(3), 237–259. https://doi.org/10.1007/s10551-005-1902-9

Andembubtob, D. R., Apuru, J. I., & Ezra, S. D. (2020). Software piracy in Nigeria. *Asian Journal of Research in Computer Science, 6*(1), 1–13. https://doi.org/10.9734/ajrcos/2020/v6i130148

Apache Software Foundation. (2004). *Apache License, version 2.0*. https://www.apache.org/licenses/LICENSE-2.0

Asongu, S. A. (2014a). Software piracy and scientific publications: Knowledge economy evidence from Africa. *African Development Review, 26*(4), 572–583. https://doi.org/10.1111/1467-8268.12113

Asongu, S. A. (2014b). Software piracy, inequality and the poor: Evidence from Africa. *Journal of Economic Studies, 41*(4), 526–553. https://doi.org/10.1108/JES-10-2012-0141

Asongu, S. A., & Andrés, A. R. (2017). The impact of software piracy on inclusive human development: Evidence from Africa. *International Review of Applied Economics, 31*(5), 585–607. https://doi.org/10.1080/02692171.2017.1296414

Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review, 3*(3), 193–209. https://doi.org/10.1207/S15327957PSPR0303_3

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy, 76*(2), 169–217. https://doi.org/10.1086/259394

Bradley, W. A., & Kolev, J. (2023). How does digital piracy affect innovation? Evidence from software firms. *Research Policy, 52*(3), 104701. https://doi.org/10.1016/j.respol.2022.104701

BSA | The Software Alliance. (2018). *Software management: Security imperative, business opportunity—2018 BSA Global Software Survey*. https://www.bsa.org/files/2019-02/2018_BSA_GSS_Report_en_.pdf

Chang, B.-H., Nam, S.-H., Kwon, S.-H., & Chan-Olmsted, S. M. (2017). Toward an integrated model of software piracy determinants: A cross-national longitudinal study. *Telematics and Informatics, 34*(7), 1113–1124. https://doi.org/10.1016/j.tele.2017.05.002

Chen, Y.-N., & Png, I. P. L. (2003). Information goods pricing and copyright enforcement: Welfare analysis. *Information Systems Research, 14*(1), 107–123. https://doi.org/10.1287/isre.14.1.107.14762

Cheng, H. K., Sims, R. R., & Teegen, H. (1997). To purchase or to pirate software: An empirical study. *Journal of Management Information Systems, 13*(4), 49–60. https://doi.org/10.1080/07421222.1997.11518142

Conner, K. R., & Rumelt, R. P. (1991). Software piracy: An analysis of protection strategies. *Management Science, 37*(2), 125–139. https://doi.org/10.1287/mnsc.37.2.125

Cronan, T. P., & Al-Rafee, S. (2008). Factors that influence the intention to pirate software and media. *Journal of Business Ethics, 78*(4), 527–545. https://doi.org/10.1007/s10551-007-9366-8

Djekic, P., & Loebbecke, C. (2007). Preventing application software piracy: An empirical investigation of technical copy protections. *Journal of Strategic Information Systems, 16*(2), 173–186. https://doi.org/10.1016/j.jsis.2007.05.005

Douglas, D. E., Cronan, T. P., & Behel, J. D. (2007). Equity perceptions as a deterrent to software piracy behavior. *Information & Management, 44*(5), 503–512. https://doi.org/10.1016/j.im.2007.05.002

Eisend, M. (2019). Explaining digital piracy: A meta-analysis. *Information Systems Research, 30*(2), 636–664. https://doi.org/10.1287/isre.2018.0821

Federal Republic of Nigeria. (2015). Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (Act No. 17). https://www.nfiu.gov.ng/images/Downloads/downloads/cybercrime.pdf

Federal Republic of Nigeria. (2023). Copyright Act, 2022 (Act No. 8, Official Gazette, 110[56], A179–A243). https://www.copyright.gov.ng/CopyrightAct/CopyrightAct2023FinalPublication1.pdf

Federal Republic of Nigeria. (2024). Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024. https://www.wipo.int/wipolex/en/legislation/details/22699

Fleming, P., Watson, S. J., Patouris, E., Bartholomew, K. J., & Zizzo, D. J. (2017). Why do people file share unlawfully? A systematic review, meta-analysis and panel study. *Computers in Human Behavior, 72*, 535–548. https://doi.org/10.1016/j.chb.2017.02.014

Free Software Foundation. (2007). *GNU General Public License (Version 3)*. https://www.gnu.org/licenses/gpl-3.0.en.html

Gan, L. L., & Koh, H. C. (2006). An empirical study of software piracy among tertiary institutions in Singapore. *Information & Management, 43*(5), 640–649. https://doi.org/10.1016/j.im.2006.03.005

Ginarte, J. C., & Park, W. G. (1997). Determinants of patent rights: A cross-national study. *Research Policy, 26*(3), 283–301. https://doi.org/10.1016/S0048-7333(97)00022-X

Givon, M., Mahajan, V., & Muller, E. (1995). Software piracy: Estimation of lost sales and the impact on software diffusion. *Journal of Marketing, 59*(1), 29–37. https://doi.org/10.1177/002224299505900103

Glass, R. S., & Wood, W. A. (1996). Situational determinants of software piracy: An equity theory perspective. *Journal of Business Ethics, 15*(11), 1189–1198. https://doi.org/10.1007/BF00412817

Gopal, R. D., & Sanders, G. L. (1998). International software piracy: Analysis of key issues and impacts. *Information Systems Research, 9*(4), 380–397. https://doi.org/10.1287/isre.9.4.380

Hinduja, S. (2001). Correlates of Internet software piracy. *Journal of Contemporary Criminal Justice, 17*(4), 369–382. https://doi.org/10.1177/1043986201017004006

Hinduja, S. (2003). Trends and patterns among online software pirates. *Ethics and Information Technology, 5*(1), 49–61. https://doi.org/10.1023/A:1024910523384

Hinduja, S. (2007). Neutralization theory and online software piracy: An empirical analysis. *Ethics and Information Technology, 9*(3), 187–204. https://doi.org/10.1007/s10676-007-9143-5

Husted, B. W. (2000). The impact of national culture on software piracy. *Journal of Business Ethics, 26*(3), 197–211. https://doi.org/10.1023/A:1006250203828

Ingram, J. R., & Hinduja, S. (2008). Neutralizing music piracy: An empirical examination. *Deviant Behavior, 29*(4), 334–366. https://doi.org/10.1080/01639620701588131

Iqbal, A., Aman, M. N., Rejendran, R., & Sikdar, B. (2024). Unveiling the connection between malware and pirated software in Southeast Asian countries: A case study. *IEEE Open Journal of the Computer Society, 5*, 62–72. https://doi.org/10.1109/OJCS.2024.3364576

Jaisingh, J. (2009). Impact of piracy on innovation at software firms and implications for piracy policy. *Decision Support Systems, 46*(4), 763–773. https://doi.org/10.1016/j.dss.2008.11.018

Kukla-Gryz, A., Tyrowicz, J., & Krawczyk, M. (2021). Digital piracy and the perception of price fairness: Evidence from a field experiment. *Journal of Cultural Economics, 45*, 105–131. https://doi.org/10.1007/s10824-020-09390-4

Kuo, F.-Y., & Hsu, M.-H. (2001). Development and validation of ethical computer self-efficacy measure: The case of softlifting. *Journal of Business Ethics, 32*(4), 299–315. https://doi.org/10.1023/A:1010715504824

Lau, E. K. W. (2003). An empirical study of software piracy. *Business Ethics: A European Review, 12*(3), 233–245. https://doi.org/10.1111/1467-8608.00323

Limayem, M., Khalifa, M., & Chin, W. W. (2004). Factors motivating software piracy: A longitudinal study. *IEEE Transactions on Engineering Management, 51*(4), 414–425. https://doi.org/10.1109/TEM.2004.835087

Logsdon, J. M., Thompson, J. K., & Reid, R. A. (1994). Software piracy: Is it related to level of moral judgment? Journal of Business Ethics, 13(11), 849–857. https://doi.org/10.1007/BF00871698

Marron, D. B., & Steel, D. G. (2000). Which countries protect intellectual property? The case of software piracy. *Economic Inquiry, 38*(2), 159–174. https://doi.org/10.1111/j.1465-7295.2000.tb00011.x

Mishra, A., Akman, I., & Yazici, A. (2006). Software piracy among IT professionals in organizations. *International Journal of Information Management, 26*(5), 401–413. https://doi.org/10.1016/j.ijinfomgt.2006.01.004

Moores, T. T., & Chang, J. C.-J. (2006). Ethical decision making in software piracy: Initial development and test of a four-component model. *MIS Quarterly, 30*(1), 167–180. https://doi.org/10.2307/25148722

Moores, T. T., & Dhillon, G. (2000). Software piracy: A view from Hong Kong. *Communications of the ACM, 43*(12), 88–93. https://doi.org/10.1145/355112.355129

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Peace, A. G., Galletta, D. F., & Thong, J. Y. L. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems, 20*(1), 153–177. https://doi.org/10.1080/07421222.2003.11045759

Peitz, M., & Waelbroeck, P. (2006). Piracy of digital products: A critical review of the theoretical literature. *Information Economics and Policy, 18*(4), 449–476. https://doi.org/10.1016/j.infoecopol.2006.06.005

Prasad, A., & Mahajan, V. (2003). How many pirates should a software firm tolerate? An analysis of piracy protection on the diffusion of software. *International Journal of Research in Marketing, 20*(4), 337–353. https://doi.org/10.1016/j.ijresmar.2003.02.001

Shadlen, K. C., Schrank, A., & Kurtz, M. J. (2005). The political economy of intellectual property protection: The case of software. *International Studies Quarterly, 49*(1), 45–71. https://doi.org/10.1111/j.0020-8833.2005.00334.x

Shy, O., & Thisse, J.-F. (1999). A strategic approach to software protection. *Journal of Economics & Management Strategy, 8*(2), 163–190. https://doi.org/10.1111/j.1430-9134.1999.00163.x

Sikolia, D., Bahr, G., & Biros, D. (2025). Software piracy: The effects of neutralization and religiosity. *The Journal of the Southern Association for Information Systems, 12*(2), 1–17. https://doi.org/10.17705/3JSIS.00038

Simpson, P. M., Banerjee, D., & Simpson, C. L., Jr. (1994). Softlifting: A model of motivating factors. *Journal of Business Ethics, 13*(6), 431–438. https://doi.org/10.1007/BF00881451

Sims, R. R., Cheng, H. K., & Teegen, H. (1996). Toward a profile of student software piraters. *Journal of Business Ethics, 15*(8), 839–849. https://doi.org/10.1007/BF00381852

Siponen, M., Vance, A., & Willison, R. (2012). New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management, 49*(7–8), 334–341. https://doi.org/10.1016/j.im.2012.06.004

Sundararajan, A. (2004). Managing digital piracy: Pricing and protection. *Information Systems Research, 15*(3), 287–308. https://doi.org/10.1287/isre.1040.0030

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664–670. https://doi.org/10.2307/2089195

Takeyama, L. N. (1994). The welfare implications of unauthorized reproduction of intellectual property in the presence of demand network externalities. *The Journal of Industrial Economics, 42*(2), 155–166. https://doi.org/10.2307/2950487

Takeyama, L. N. (1997). The intertemporal consequences of unauthorized reproduction of intellectual property. *The Journal of Law and Economics, 40*(2), 511–522. https://doi.org/10.1086/467382

Tang, J.-H., & Farn, C.-K. (2005). The effect of interpersonal influence on softlifting intention and behaviour. *Journal of Business Ethics, 56*(2), 149–161. https://doi.org/10.1007/s10551-004-2170-9

Wagner, S. C., & Sanders, G. L. (2001). Considerations in ethical decision-making and software piracy. *Journal of Business Ethics, 29*(1–2), 161–167. https://doi.org/10.1023/A:1006415514200

Wolfe, S. E., Higgins, G. E., & Marcum, C. D. (2008). Deterrence and digital piracy: A preliminary examination of the role of viruses. *Social Science Computer Review, 26*(3), 317–333. https://doi.org/10.1177/0894439307309465

World Trade Organization. (1994). Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization. https://www.wto.org/english/docs_e/legal_e/27-trips.pdf