

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL NO. 1157



Introduced by **REP. JAVIER MIGUEL L. BENITEZ**

EXPLANATORY NOTE

Republic Act ("RA") No. 4200 (1965), or the Anti-Wiretapping Law of 1965, was a legislation that sought to uphold the constitutional right to privacy of communication. At the time of its passage, the threats to communication privacy were limited to analog devices such as wiretaps, tape recorders, and other basic surveillance equipment.¹ Nearly six decades later, the rapid and continuous evolution of technology has rendered the law increasingly inadequate and outdated.

In today's digital age, the threats to communication privacy have expanded far beyond physical wiretapping. Advanced surveillance tools such as spyware, malware, artificial intelligence-powered monitoring systems, and voice or facial recognition technologies can now intercept, store, and analyze personal conversations without consent or knowledge.² With the increasing digital innovations, digital wiretapping may also be abused by attackers to target the data of the users and leverage it according to their personal interests.³ Even everyday used devices like smartphones, smartwatches, and laptops are capable of being transformed into surveillance instruments.⁴ Worse, these tools are accessible not only to state agents but also to private actors and malicious entities.

The amended bill seeks to modernize and expand the scope of RA No. 4200 to include newer forms of communication such as digital, electronic, and internet-based, while also prohibiting the unauthorized use of modern surveillance

¹ Republic Act No. 4200 Anti-Wiretapping Act (1965)

² Brewster, T. (2024). The Wiretap: AI Is Already Supercharging Cyberattacks, Warns Government Minister. *Forbes*. <https://www.forbes.com/sites/thomasbrewster/2024/12/03/the-wiretap-ai-is-already-supercharging-cyberattacks-warns-government-minister/>

³ Twingate (2024). What is Wiretapping? How it Works and Examples. <https://www.twingate.com/blog/glossary/wiretapping>

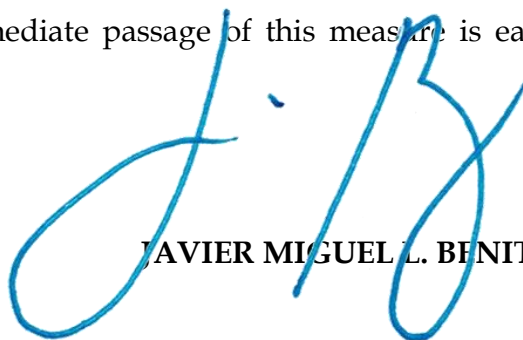
⁴ Pippig, L. (2024). Do smartphones eavesdrop on conversations? New evidence says yes. *PC World*. <https://www.pcworld.com/article/2450052/do-smartphones-listen-to-everything-new-evidence-speaks-in-favour.html>

technologies. It introduces provisions that criminalize the use of Artificial Intelligence (AI) and automated systems for eavesdropping, adds stricter penalties, clarifies the meaning of consent, and mandates judicial safeguards against abuse.

The amended legislation recognizes the importance of balancing national security interests with the protection of individual rights and liberties. While the law maintains an exception for court-authorized surveillance for serious crimes, it tightens the rules to ensure that such powers are not abused and that due process is always observed.

As the Philippines moves further into a highly interconnected digital society, the laws must evolve to keep up with both the opportunities and the threats posed by innovation. The Expanded Anti-Wiretapping and Digital Surveillance Prevention Act of 2025 ensures that Filipinos' right to privacy remains protected online, offline, and across all forms of communication.

In view of the foregoing, the immediate passage of this measure is earnestly sought.



JAVIER MIGUEL L. BENITEZ

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL NO. 1157

Introduced by **REP. JAVIER MIGUEL L. BENITEZ**

**AN ACT AMENDING REPUBLIC ACT NO. 4200, OTHERWISE
KNOWN AS THE ANTI-WIRETAPPING LAW OF 1965, TO INCLUDE NEW
TECHNOLOGIES AND MODERN SURVEILLANCE METHODS, AND FOR
OTHER PURPOSES**

*Be it enacted by the Senate and the House of Representatives of the Philippines in
Congress assembled:*

SECTION 1. *Short Title* - This Act shall be known as the “*Expanded Anti-
Wiretapping and Digital Surveillance Prevention Act of 2025.*”

SEC. 2. *Declaration of Policy.* - It is the policy of the State to protect the
privacy and dignity of every individual against perpetrators. In recognition of
evolving communication technologies, the State shall strengthen legal safeguards
against unauthorized interception, monitoring, recording, and disclosure of
private communications by any person, whether public or private, and regardless
of the medium used.

SEC. 3. A new section is hereby inserted after Section 1 of Republic Act
(“RA”) No. 4200 (1965) to be known as Section 1-A, to read as follows:

“Section 1-A. Use of Artificial Intelligence and Automated Systems.

The use of artificial intelligence (AI) systems, bots, algorithms, or
any automated technology to collect, analyze, or intercept private
communications without the explicit consent of all parties involved is
hereby prohibited.

This includes but is not limited to data scraping, keyword logging, voice cloning, and facial recognition used for surveillance or monitoring purposes.”

SEC. 4. A new section is hereby inserted after Section 1-A of RA No. 4200 to be known as Section 1-B, to read as follows:

“Section 1-B. Definition of Terms. – For purposes of this Act, the following terms shall be defined as follows:

- (a) Wiretapping – the act of secretly listening to, intercepting, recording, or monitoring private communications, whether analog or digital, without the consent of all parties involved, through any means or device.
- (b) Digital Wiretapping – the unauthorized interception or access to electronic communications using digital tools such as spyware, malware, or other hacking methods that allow the monitoring of messages, calls, emails, and other data transmissions.
- (c) Communication – any spoken word, conversation, message, data, video, or image transmitted through any medium, including but not limited to telephones, mobile phones, email, chat applications, social media, radio, VoIP, or online conferencing platforms.
- (d) Device – any instrument, equipment, software, or hardware such as telephones, mobile phones, laptops, smartwatches, surveillance cameras, microphones, routers, and digital applications, capable of recording, transmitting, intercepting, or monitoring communications.
- (e) Surveillance – the act of observing, listening, tracking, or monitoring a person or group’s communication or behavior, especially in a covert or unauthorized manner.
- (f) Malware – malicious software designed to infiltrate, damage, or gain unauthorized access to a computer system or device, often used for spying or stealing information.

- (g) Spyware – a type of malware specifically intended to secretly gather information from a device, including monitoring keystrokes, messages, and audio-visual data.
- (h) Packet Sniffing – the process of intercepting and analyzing data packets traveling over a digital network, often used to capture private information without authorization.
- (i) Consent – the explicit, voluntary, and informed agreement by all parties to a communication to allow the interception or recording of such communication. Implied or passive consent is not considered valid under this Act.
- (j) Encryption – the process of encoding information in such a way that only authorized parties can access it, used to protect communications from unauthorized interception.
- (k) Artificial Intelligence Surveillance – the use of machine learning algorithms, AI tools, or automated software to detect, monitor, analyze, or profile individuals or groups based on intercepted or collected communications or behaviors.
- (l) Metadata – data that provides information about other data, including time, location, sender, recipient, and device details related to a communication, even if the content itself is not intercepted. For the purposes of this Act, metadata shall be treated as protected communication content when it can reasonably reveal personal or sensitive information.
- (m) Court Order – a written authorization issued by a competent court, based on probable cause, permitting specific surveillance activities within the scope defined by this Act.

SEC. 5. Section 1 of the RA No. 4200 is hereby amended to read as follows:

"Section 1. It shall be unlawful for any person, not being authorized by all parties to any private communication or spoken word, to tap any wire or cable, or by using any other device or digital means, to secretly overhear, intercept, monitor, collect, record, store, or transmit such

communication or spoken word, whether in analog or digital format, and regardless of platform or transmission medium.

This includes but is not limited to the use of:

- (a) Dictaphones, walkie-talkies, tape recorders;
- (b) Mobile phones, smartphones, smartwatches;
- (c) Spyware, malware, keystroke loggers;
- (d) Surveillance cameras, microphones, webcams, drones;
- (e) Artificial intelligence (AI)-enabled monitoring systems;
- (f) Internet-based applications such as emails, instant messaging platforms, video conferencing tools, or social media applications;
- (g) Voice-over-IP (VoIP) and cloud-based communication systems.

when such devices are primarily or intentionally used for unauthorized interception.

It shall likewise be unlawful to manufacture, import, distribute, sell, or advertise devices or software primarily designed to intercept communications without lawful authority.

Possession, storage, use, transmission, dissemination, or replay of any unauthorized recordings obtained through any of the aforementioned means shall be punishable under this Act, unless explicitly exempted by law.

Provided, however, that this Act shall not apply to recordings or interceptions made by journalists, whistleblowers, or concerned individuals acting in good faith and without malice to expose corruption, abuse of authority, or violations of law, provided that such actions are subject to judicial determination and consistent with public interest and due process."

SEC. 6. Section 2 of RA No. 4200 is hereby amended to read as follows:

"Section 2. Any person who violates Section 1 or Section 1-A of this Act shall be punished with:

- (a) Imprisonment of six (6) to twelve (12) years;
- (b) A fine of not less than Five Hundred Thousand Pesos (₱500,000.00) but not more than One Million Pesos (₱1,000,000.00);

- (c) Perpetual absolute disqualification from holding public office if the offender is a public official; and
- (d) Deportation, if the offender is an alien.

If the offense involves a government surveillance program conducted without any court order, the penalty shall be reclusion temporal, and all evidence obtained shall be inadmissible."

SEC. 7. *Inclusion of Digital Consent requirement -*

"No recording or surveillance shall be considered authorized unless all parties have given explicit, recorded, and verifiable consent in accordance with Republic Act No. 10173 or the Data Privacy Act of 2012. Implied or passive consent shall not suffice."

SEC. 8. Section 3 of the RA No. 4200 is hereby amended to read as follows:

Following the provisions of this Act, it shall not be unlawful for a duly authorized peace officer to conduct surveillance, intercept, record, or overhear private communications, conversations, discussions, or spoken words, provided that:

- (a) Such surveillance is authorized by a written order issued by the Regional Trial Court ("RTC") having territorial jurisdiction over the place where the surveillance will be conducted;
- (b) The application for the court order must be in writing and shall be granted only after:
 - (1) Examination under oath or affirmation of the applicant and any supporting witnesses;
 - (2) A finding that there are reasonable grounds to believe that any of the following crimes has been committed, is being committed, or is about to be committed:
 - (i) Treason
 - (ii) Espionage
 - (iii) Provoking war and disloyalty in case of war
 - (iv) Piracy or mutiny on the high seas
 - (v) Rebellion or insurrection

(vi) Conspiracy or proposal to commit rebellion

(vii) Inciting to rebellion

(viii) Sedition

(ix) Conspiracy or proposal to commit sedition

(x) Inciting to sedition

(xi) Kidnapping, as defined in the Revised Penal Code

(xii) Violations of Commonwealth Act No. 616 or other offenses against national security;

(3) A document showing that evidence to be obtained is essential to convicting the suspect, solving the case, or preventing the crime; and

(4) A document showing that no other method is readily available to obtain such evidence.

(c) In cases of rebellion, proposal or conspiracy to commit rebellion, sedition, and inciting to sedition, surveillance shall only be allowed upon prior proof that rebellion or acts of sedition are actually being committed or have occurred. The court order must clearly state:

(1) The identity of the person(s) whose communications are to be monitored;

(2) In the case of telephonic or telegraphic communications, the specific phone number or communication line and its location;

(3) The identity of the peace officer authorized to perform the surveillance;

(4) The offense(s) involved; and

(5) The authorized duration, not to exceed sixty (60) days from the date of issuance, unless extended by the court for valid public interest.

(d) All recordings made pursuant to the court order shall be deposited with the issuing court within forty-eight (48) hours after the expiration of the authorized period. The deposit shall be:

- (1) Sealed in an envelope or package; and
- (2) Accompanied by a sworn affidavit of the authorized officer, indicating:
 - (i) The number of recordings,
 - (ii) The dates and times covered,
 - (iii) The number and type of storage media used, and
 - (iv) A certification that no duplicates exist

(e) The contents of said recordings shall remain confidential and may only be accessed, replayed, or presented as evidence upon a separate court order, issued with notice and opportunity to be heard by the person(s) whose communications were recorded.

(f) The term "court" as used in this section refers to the RTC with jurisdiction over the location where the surveillance will be executed.

SEC. 9. Section 4 of Republic Act No. 4200 is hereby amended to include:

"No communication or data obtained through unauthorized or unlawful surveillance, digital or analog, shall be admissible in evidence in any proceeding, and any copies thereof shall be destroyed by court order."

SEC. 10. *Monitoring and Evaluation body* - To ensure accountability and transparency, the Department of Justice shall conduct regular monitoring and evaluation of the implementation of this Act in coordination with the National Privacy Commission ("NPC"), Commission on Human Rights ("CHR"), and Department of Information and Communications Technology ("DICT").

All government agencies or entities authorized to conduct surveillance under this Act shall be required to submit periodic reports to the Department of Justice ("DOJ"). These reports shall include, but shall not be limited to, the following:

- (a) Monitoring the use of surveillance technologies;
- (b) Investigating abuses committed under this Act;
- (c) Submitting an annual report with recommendations to improve legislation and implementation;
- (d) Reviewing all court-approved wiretaps;

- (e) Issuing compliance orders or recommend prosecution, where applicable; and
- (f) Monitoring and assessing evolving technologies related to eavesdropping

SEC. 11. *Implementing Rules and Regulations* - The DOJ, in coordination with the DICT, The NPC, the CHR, shall promulgate the implementing rules and regulations necessary for the effective implementation of this Act within ninety (90) days from its effectivity.

SECTION 12. *Appropriations*. - The amount necessary to carry out the provisions of this Act is hereby authorized to be appropriated in the concerned agencies in the General Appropriations Act for the year following its enactment into law and thereafter.

SECTION 13. *Repealing Clause* - All laws, presidential decrees, executive orders, rules and regulations inconsistent with the provisions of this Act are hereby repealed or modified accordingly.

SECTION 14. *Separability Clause* - If any provision of this Act is declared unconstitutional, the remainder shall not be affected thereby.

SECTION 15. *Effectivity* - This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation.

Approved,