

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

Sixteenth Congress
First Regular Session

HOUSE BILL NO. **3097**



Introduced by Honorable Arthur R. Defensor, Jr.

EXPLANATORY NOTE

The right to privacy had been long recognized as among the fundamental rights that inhere to every person by virtue solely of his humanity. Indeed, it is a right most valued by civilized men that commands respect in any jurisdiction governed by the rule of law. Under Sections 2 and 3 of the Bill of Rights in our Constitution, the right to privacy is held sacred by commanding:

“Section 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant and warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.

Section 3. (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law.

(2) Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.”

To preserve the enjoyment of such right by the people, the Anti-Wiretapping Law was enacted by Congress on 19 June 1965, almost fifty (50) years ago. Since then, the unstoppable advancement of information and communication technology has operated to diminish traditional zones of privacy enjoyed by the people. The coming of the digital age ushered in an era of unprecedented convenience and interconnectivity

which revolutionized the life of the ordinary Filipino. The developments in technology proliferated seemingly benign and innocuous devices which coupled by malice and mischief, possess the potential to undermine the very civil liberties held dear in our democratic society.

Unfortunately, the law has failed to keep a pace of the continuously evolving realities thrust upon us by the technologies achieved by human ingenuity. Moreover, the interest of government in maintaining security, peace, and order, as well as the indiscriminate enforcement of the law demand equal consideration for these interests are likewise essential in any civilized and democratic society.

At present, there are four (4) modes by which an individual may communicate with others: (1) oral, (2) written, (3) wire, and (4) electronic communications. With the exception of written communications, all these modes are ephemeral and non-corporeal in character and for this reason, are easily susceptible to interception, reproduction, and disclosure with the numerous digital devices possessing an incidental capacity to do so.

This Bill seeks to improve the old Anti-Wiretapping law by expanding the general prohibition to the interception and disclosure of oral, wire, and electronic communications. It provides for adaptable statutory standards designed to address future advancements and developments in information and communication technology. It likewise seeks to strike a delicate balance between the competing yet, equally compelling, interest to the right to privacy of individuals and the maintenance of peace and order and law enforcement by drawing concepts from the Electronic Communications Privacy Act (18 U.S.C. 2510-2522) of the United States of America.

The foregoing duly considered, the approval of this bill is earnestly sought.



ARTHUR R. DEFENSOR, JR.

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

SIXTEENTH CONGRESS
First Regular Session

HOUSE BILL NO. **3097**

Introduced by Representative Arthur R. Defensor, Jr.

AN ACT
PROHIBITING THE INTERCEPTION AND DISCLOSURE OF ORAL, WIRE,
OR ELECTRONIC COMMUNICATIONS AND OTHER VIOLATIONS OF THE
RIGHT TO PRIVACY OF COMMUNICATION AND FOR OTHER PURPOSES

1 **Section 1. *Short Title.*** - This Act shall be known as the "Privacy of
2 Communications Act".
3

4 **Section 2. *Declaration of Policy.*** - It is the policy of the State to ensure the
5 inviolability of the right of the people to be the privacy of communication and
6 correspondence as provided by the 1987 Constitution. However it is likewise
7 recognized that such right is not absolute in view of other equally compelling state
8 interests such as the right of the State to investigate, prosecute, and punish violators
9 of the law. Accordingly, such right of privacy may be overcome by lawful order of
10 the court, or when public safety or order requires as provided by law.
11

12 As new technologies continue to be discovered and become commonplace in
13 an ever increasingly digitalized world, it is recognized that the law must ever keep
14 apace in evaluating its impact on privacy rights and to ensure that the right of
15 privacy enjoyed by the people is adequately guaranteed by law.
16

17 **Section 3. *Declaration of Terms.*** - For the purposes of this Act, unless the
18 context indicates otherwise:
19

20 (a) "Aggrieved person" refers to any person, natural or juridical,
21 whose communications, whether wire, oral, or electronic, were intercepted in
22 violation of the provisions of this Act.
23

24 (b) "Contents" as used in this Act and when used with respect to
25 any wire, oral, or electronic communication, includes any information
26 concerning the substance, purport, or meaning of that communication.
27

28 (c) "Court of competent jurisdiction" refers to any regional trial
29 court, the Court of Tax Appeals, Court of Appeals, Sandiganbayan, and the
30 Supreme Court having or in the exercise of lawful jurisdiction under the law
31 and the Constitution.
32

33 (d) "Electronic communication" refers to any communication made
34 in whole through the means of electronic data messages or electronic
35 documents as defined by Republic Act No. 8792 and the Rules on Electronic
36 Documents and regardless of the form of output thereof.
37

38 (e) "Electronic, mechanical, or other communication intercepting
39 device" means any device or apparatus whose primary purpose is the
40 surreptitious interception of a wire, oral, or electronic communication as
41 defined by this Act other than—
42

43 (1) any telephone, cellular phone, or telegraph instrument,
44 equipment or facility, or any component thereof,
45

46 (i) furnished to the subscriber or user by a provider of
47 wire or electronic communication service in the ordinary course of
48 its business and being used by the subscriber or user in the
49 ordinary course of its business or furnished by such subscriber or
50 user for connection to the facilities of such service and used in the
51 ordinary course of its business; or
52

53 (ii) being used by a provider of wire or electronic
54 communication service in the ordinary course of its business, or by
55 an investigative or law enforcement officer in the ordinary course
56 of his duties;
57

58 (2) a hearing aid or similar device being used to correct subnormal
59 hearing to not better than normal.
60

61 (f) "Intercept" refers to the acquisition of the contents, either in
62 whole or in part, of any wire, electronic, or oral communication through the
63 use of any electronic, mechanical, or other device.
64

65 (g) "Investigative or law enforcement officer" means any officer or
66 agent of the Republic of the Philippines or any political subdivision thereof,
67 who is empowered by law to conduct investigations of or to make arrests for
68 criminal offenses penalized by law, and any attorney authorized by law to
69 prosecute or participate in the prosecution of such offenses.

(h) "Oral communication" refers to any communication uttered, spoken, or otherwise made by gestures, facial expressions and such other communication not expressed in writing by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication as defined by this Act.

(i) "Wire communication" refers to any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

(j) "Computer trespasser" –

(1) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(2) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

Section 4. Coverage. – This Act shall cover all oral, wire, and electronic communications made in whole or in part within the territorial jurisdiction of the Republic of the Philippines.

Section 5. Prohibition against Interception of Communication. – The act of intercepting or attempting to intercept any wire, oral, or electronic communication covered by this Act made by and between any person shall be prohibited and penalized in accordance with Section __ of this Act.

Section 6. Exceptions to the Prohibition against Interception of Communication. – Except as otherwise provided by law, the following shall be excepted from the prohibition provided in the immediately preceding Section:

(a) Any interception of communication made pursuant to a lawful surveillance conducted in accordance with the provisions of this Act;

(b) Any interception of communication made by an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication made in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service public shall not utilize service observing or random monitoring except for mechanical or service quality control checks;

(c) Any interception of communication made by a person acting pursuant to or in connection with a lawful surveillance or criminal investigation made by investigative or law enforcement officers in accordance with the provisions of this Act, where such person is a party to the communication;

(d) Any interception of communication made where one of the parties to the communication has given prior consent to such interception;

(e) Any interception of electronic communication made through an electronic communication system that is readily accessible to the general public;

(f) Any interception of electronic communication by radio which

(1) Is transmitted by any station for the use of the general public;

(2) Relates to ships, aircraft, vehicles, or persons in distress or by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system readily accessible to the general public;

(3) Is made by a station operating on an authorized frequency within the bands allocated to or made available to the general public; and

(4) Is made by any marine or aeronautical communications system.

(g) Any interception of communication made by a person acting under color of law of a computer trespasser transmitted to, through, or from a computer which is protected from unwarranted or unlawful access by its owner or operator protected computer; *Provided that:*

161 (1) The owner or operator of the protected
162 computer authorizes the interception of the computer
163 trespasser's communications on the protected computer;
164

165 (2) The person making the interception is engaged
166 in lawful surveillance or criminal investigation in
167 accordance with the provisions of this Act; and
168

169 (3) Such interception does not acquire
170 communications other than those transmitted to or from the
171 computer trespasser.
172

173 **Section 7. Prohibition against Disclosure of Intercepted Communication.** - The act
174 of intentionally disclosing or who attempts to disclose to any person other than the
175 intended recipient the contents of any wire, oral, or electronic communication
176 obtained in violation of this Act shall be prohibited and penalized in accordance
177 with Section __ of this Act.
178

179 The act of disclosing or attempting to disclose to any person other than the
180 intended recipient the contents of any wire, oral, or electronic communication
181 properly obtained pursuant to lawful surveillance or criminal investigation in
182 accordance with this Act with intent to improperly obstruct, impede, or interfere
183 with such lawful surveillance or criminal investigation, shall be prohibited and
184 penalized in accordance with Section __ of this Act.
185

186 **Section 8. Exceptions to Prohibition against Disclosure of Intercepted Communication.**
187 - Except as otherwise provided by law, the following shall be excepted from the
188 prohibition provided in the immediately preceding Section:
189

190 (a) Where the disclosure of the intercepted communication is made
191 with the consent of the originator or any addressee or intended recipient of
192 such communication; and
193

194 (b) Where the disclosure of the intercepted communication is made
195 to a person employed or authorized, or whose facilities are used, to forward
196 such communication to its destination.
197

198
199 **Section 9. Prohibition against the Manufacture of Wire, Oral, or Electronic**
200 **Communication Intercepting Devices.** - The manufacture or assembly of a device whose
201 primary use, purpose, or function is the surreptitious interception of wire, oral, or
202 electronic communications shall be prohibited and penalized in accordance with
203 Section __ of this Act, except when such person who engages in the manufacture or
204 assembly of a device as defined by this Section obtains the written approval of the
205 National Telecommunications Commission (NTC).
206

Section 10. Prohibition against the Possession of Wire, Oral, or Electronic Communication Intercepting Devices. - The possession by a person of an electronic, mechanical, or other communications intercepting device without a prior written approval from the NTC and after payment of proper registration fees therefore shall be prohibited and penalized in accordance with Section __ of this Act; *Provided that*, no such registration fees shall be charged for wire, oral, or electronic communication intercepting devices procured by an investigative or law enforcement officer as defined by this Act.

Section 11. Habeas Data as Remedy against Illegal Interception of Communication. - Upon a showing that any person is engaged or is about to engage in any act which constitutes a violation or tends to violate the provisions of this Act, the aggrieved party may file, before a court of competent jurisdiction, a petition for the issuance of a writ of *habeas data* to enjoin the act complained of, or to order the deletion or destruction of the communication illegally intercepted. Such court may likewise issue a writ of injunction, whether preliminary or final, and grant any such reliefs as may be just and equitable under the circumstances.

Section 12. Recovery of Civil Damages. - Any person whose wire, oral, or electronic communication had been intercepted, disclosed, or intentionally used in violation of this Act may file a civil action for recovery of damages from the person or entity, other than the Republic of the Philippines or any of its departments, agencies, or political subdivisions, which engaged in such unlawful act.

Section 13. Statute of Limitations. - An action for civil liability pursuant to the immediately preceding Section must be filed within two years from the date the plaintiff knew or reasonably should have known the illegal interception of communication or illegal use or disclosure of such communication intercepted.

Section 14. Administrative Liability. - Any act or omission committed by an officer, employee, or agent of the Republic of the Philippines or any of its departments, agencies, or political subdivisions which constitutes a violation of this Act shall constitute grave misconduct or conduct prejudicial to the best interest of the service and accordingly be grounds for administrative liability pursuant to pertinent rules and regulations governing the Civil Service; *Provided that*, nothing in this Section shall be construed to preclude or prevent the filing of appropriate criminal charges against such officer, employee, or agent for a violation of this Act.

Section 15. Assistance to Lawful Surveillance or Criminal Investigation. - Notwithstanding any contrary provision of law, investigative or law enforcement officers are hereby authorized to intercept oral, wire, or electronic communication pursuant to a lawful surveillance or criminal investigation; *Provided that*, no interception of communication pursuant to a lawful surveillance or criminal investigation shall be allowed without an order by a court of competent jurisdiction based probable cause to be determined personally by the judge after examination under oath or affirmation of the applicant and the witnesses he may produce,

253 particularly describing the place and persons subject of the surveillance; *Provided*
254 *further*, that such order shall clearly delineate the extent, scope, and limits of the
255 surveillance.

256
257 Providers of wire or electronic communication service, their officers,
258 employees, and agents, landlords, custodians, or other persons, are authorized to
259 provide information, facilities, or technical assistance to persons authorized to
260 intercept wire, oral, or electronic communications in accordance with this Section;

261
262 **Section 16. Exclusionary Rule.** – Any form of communication obtained or
263 secured in violation of or non-compliance with the procedures provided by this Act
264 and its implementing rules and regulations by any investigative or law enforcement
265 officer shall not be admissible in evidence in any judicial, quasi-judicial, legislative
266 or administrative hearing or investigation.

267
268 **Section 17. Penal Provisions.** – Any person who knowingly or wilfully violates
269 the provisions of this Act shall be punished by imprisonment of not less than six (6)
270 months to not more than six (6) years or a fine of not less than One Hundred
271 Thousand Pesos (P100,000) and not more than Five Hundred Thousand Pesos
272 (P500,000).

273
274 **Section 18. Non-applicability to written communication.** – Notwithstanding any
275 provision of this Act to the contrary, this Act shall not apply to any communication
276 made in writing or communicated through the means of any material containing
277 letters, words, numbers, figures, symbols or other modes of written expression.

278
279 **Section 19. Implementing Rules and Regulations.** – The Department of Justice
280 (DOJ), DILG, DOTC, and DND, shall provide the necessary implementing rules and
281 regulations within thirty (30) days upon the approval of this Act and after its
282 publication in at least two (2) newspapers of general circulation.

283
284 **Section 20. Repealing Clause.** – All provisions of laws and rules inconsistent
285 with the provisions of this Act are hereby repealed or amended accordingly.

286
287 **Section 21. Separability Clause.** – If, for any reason, any section or provision of
288 this Act is declared unconstitutional or invalid, the other sections or provisions not
289 affected thereby shall remain in full force and effect.

290
291 **Section 22. Effectivity Clause.** – This Act shall take effect after fifteen (15) days
292 following its publication in a newspaper of general circulation.