

Title	The Communication Security and Surveillance Act
Amended Date	2014.01.29
Category	Ministry of Justice (法務部)

Article 1 This Act is enacted to

safeguard the freedom of

private communications

and privacy, to protect from

unlawful intrusion, and to

ensure national security

and maintain social order.

Article 2 Communication

surveillance may only be

conducted for the necessity

of ensuring national

security, and maintaining

social order.

The surveillance mentioned

in the preceding Paragraph

shall not exceed the

necessary limits to achieve
the objective, and the
appropriate methods for
the action should have only
the minimum intrusion.

Article 3

The "communications" as
defined in this Act refer to:

1. Utilizing wired and

wireless

telecommunication

equipment to send, store,

transmit, or receive

symbols, texts, images,

sound or other types of

information.

2. Mail and letters

3. Speeches and

conversations.

Surveillance of the

"communications"

mentioned in the preceding

Paragraph is limited to

those who have sufficient

facts to support that those

being monitored have

reasonable expectations

that the contents of their

communications are private

or secret.

Article 3-1

The "communications

records" as defined in this

Act refer to records such as

the telecommunications

numbers of the sender and

the recipient, time of

communication, length of

use, address, service type,
mailbox or location
information generated by
the telecommunications
system after the
telecommunications user
uses the
telecommunications
services.

The “communications
user’s information” as
defined in this Act refers to
the telecommunications
user’s name, number of
identification document,
telecommunications
number and information
completed in the
application, for any type of

telecommunications

service.

Article 4

Persons under surveillance

as defined in this Act

include, in addition to those

delineated in the provisions

of Article 5 and Article 7,

those who assist in

sending, transmitting,

receiving communications

or those who provide

communication equipment,

or facilities.

Article 5

An interception warrant

may be issued, if there is

sufficient evidence that the

accused or the suspect is

involved in one of the

following crimes, which
may severely endanger
national security, economic
order or social order, and
that there is reasonable
belief that the content of
his/her communication is
relevant to the case being
investigated, and that it is
difficult or there are no
other methods to collect or
investigate the evidence.

1. The offenses are
punishable with a minimum
of a three-year fixed-term
imprisonment.

2. Offenses as stipulated in
Article 100, Paragraph 2
preparing to commit civil

disturbance, Article 101,
Paragraph 2 preparing to
commit civil disturbance
with force, or Article 106,
Paragraph 3; Article 109,
Paragraphs 1, 3 and 4;
Article 121, Paragraph 1;
Article 122, Paragraph 3;
Article 131, Paragraph 1;
Article 142; Article 143,
Paragraph 1, Article 144;
Article 145; Article 201-1;
Article 256, Paragraphs 1
and 3; Article 257,
Paragraphs 1 and 4; Article
298, Paragraph 2; Article
300; Article 339; Article
339-3 or Article 346 of the
Criminal Code.

3. Offenses of corruption

for breach of official duty as

stipulated in Article 11,

Paragraphs 1 and 4 of the

Anti-Corruption Act.

4. Offenses as stipulated in

Article 2, Paragraphs 1 and

2, or Article 3 of the

Smuggling Penalty Act.

5. Offenses as stipulated in

Article 82, Paragraphs 1

and 4, or Article 83

Paragraphs 1 and 4 of the

Pharmaceutical Affairs Act.

6. Offenses as stipulated in

Article 173 Paragraph 1 of

the Securities and

Exchange Act.

7. Offenses as stipulated in

Article 112, or Article 113

Paragraphs 1 and 2 of the

Futures Trading Act.

8. Offenses as stipulated in

Article 12, Paragraphs 1, 2,

4 and 5, or Article 13,

Paragraph 2, 4 and 5 of the

Act Governing the Control

and Prohibition of Guns,

Cannon, Ammunition, and

Knives.

9. Offenses as stipulated in

Article 102, Paragraph 1,

Subparagraph 1 of the Civil

Servants Election and

Recall Act.

10. Offenses as stipulated

in Article 47-1 or Article

47-2 of the Farmers

Association Act.

11. Offenses as stipulated

in Article 50-1, or Article

50-2 of the Fishermen

Association Act.

12. Offenses as stipulated

in Article 23, Paragraphs 1,

3, 4, and 5 of the Child and

Youth Sexual Transaction

Prevention Act.

13. Offenses as stipulated

in Article 11, Paragraphs 1

to 3 of the Money

Laundering Control Act.

14. Offenses as stipulated

in Article 3, second half of

Paragraph 1, second half of

Paragraph 2; Article 6 or

Article 11, Paragraph 3 of

the Organized Crime

Prevention Act.

15. Offenses as stipulated

in Article 14, Paragraph 2;

Article 17, Paragraph 3;

Article 18, Paragraph 3;

Article 19, Paragraph 3;

Article 20, Paragraph 5;

Article 22, Paragraph 4;

Article 23, Paragraph 3;

Article 24, Paragraphs 2

and 4; Article 58,

Paragraph 5, or Article 63,

Paragraph 1 of the Criminal

Code of the Armed Forces.

16. Offenses as stipulated

in Article 13-2, Paragraphs

1 and 2 of the Trade

Secrets Act.

17. Offenses as stipulated
in Article 52, Paragraphs 1
and 2 of the Forestry Act.

18. The offense as
stipulated in Article 46 of
the Waste Disposal Act.

The interception warrant
mentioned in the preceding
Paragraph shall be applied
for, during the
investigation, by the
prosecutor upon receiving
applications from judicial
police authorities, or
applied by the prosecutor
ex officio to the court
concerned for issuance.

The application shall
specify the case numbers

starting with the words
“Zheng” and “Tang” and
information delineated in
Article 11, and the reasons,
along with relevant
documents. If the target of
interception is not a user of
a telecommunications
service, it should be
specified in the application.
Relevant documents and
investigation information
about the residence of the
target of interception
should also be attached,
specifying that there is
sufficient reason to believe
that the contents of
communications are

related to the case, that
prior investigation has been
conducted in another
manner without success, or
that it is reasonably clear
that investigation in another
manner will not achieve the
purpose or creates material
risk. The prosecutor should
respond within four hours
after accepting the
application. If the case is
complex, the deadline may
be extended for four hours
with the consent of the
Chief Prosecutor. The court
should reply within 48
hours after receiving the
application case as

approved by and transferred from the prosecutor. If the case is in trial proceedings, the warrant should be issued ex officio by the judge. The judge may also enter appropriate instructions to the enforcement officers on the interception warrant.

If the application as referred to in the preceding Paragraph is inconsistent with the legal procedure, lacks reason, is not specified or not sufficiently specified, it shall be denied by the court. The decision to deny an application by

the court shall not be
challenged.

The enforcement authority
shall file at least one report
every 15 days during the
period of communication
surveillance, describing the
progress of conducting the
surveillance, and/or if there
is the necessity to continue
implementing the
surveillance. The
prosecutor or the judge that
issued the interception
warrant may also order the
enforcement authority to
submit a report at any time.
If a situation arises where
the surveillance should not

be conducted continuously,
the judge shall consider, by
free evaluation based on
the rules of experience and
logic, withdrawing the
issued interception warrant.

The application for
interception warrant shall
be limited to the same
target, under the same
case number starting with
the words “Zheng” and
“Tang” or related cases. An
application may be filed to
seek several interception
warrants.

Article 6

If there are sufficient facts
to support that the accused

or the suspect is
committing the offenses of
interference with voting as
stated in the Criminal
Code; the offenses as
stipulated in the Civil
Servants Election and
Recall Act, the Presidential
and Vice Presidential
Election and Recall Act,
Articles 7 and 8 of the Act
Governing the Control and
Prohibition of Guns,
Cannon, Ammunition, and
Knives, Article 4 of the
Narcotics Hazard
Prevention Act; the
offenses of Extortion and
Kidnapping for Ransom, or

the offenses of Extortion by
means of using bombs,
explosives, or poison;
offenses as stipulated in
Article 3 of the Organized
Crime Prevention Act,
Article 11, Paragraphs 1, 2
and 3 of the Money
Laundering Control Act,
Article 222, Article 226,
Article 271, Article 325,
Article 326, Article 328,
Article 330, Article 332, or
Article 339 of the Criminal
Code, in order to protect
people's lives, bodies, or
property from immediate
harm, or there are facts
justifying the existence of

other communications that
are used for contact in
order to commit the
offenses under Paragraph
1 of the previous Article
and the situation is urgent,
the judicial police authority
may report to the
prosecutor concerned, who
will then verbally inform the
enforcement authority to
give priority to the
communication
surveillance. However, the
prosecutor should inform
the enforcement authority
of the content as
delineated in Article 11,
and report to the court

concerned within 24 hours
and request the issuance of
an interception warrant; the
prosecutorial agency
should designate a Head
Prosecutor, or a
prosecutor, as an
emergency contact to
facilitate the investigation in
a timely manner.

The court should designate
a specific communication
contact to handle the case,
and should issue an
interception warrant within
48 hours; if an interception
warrant is not issued within
48 hours, the surveillance
activity should be halted.

Article 7

When it is necessary to
conduct surveillance on the
following communications
in order to collect
intelligence on foreign
forces or hostile foreign
forces to protect national
security, the head of the
authority overseeing
national intelligence may
issue the interception
warrant.

1. Domestic

communications of foreign
forces, hostile foreign
forces, or their agents.

2. Cross-border

communications of foreign
forces, hostile foreign

forces, or their agents.

3. Off-shore

communications of foreign

forces, hostile foreign

forces, or their agents.

The issuance of an

interception warrant for

persons under the

communication

surveillance as described

in the preceding

Paragraph, who have a

registered permanent

address within the country,

should be approved by the

dedicated judge of the high

court that has jurisdiction

over the authority

overseeing national

intelligence. However, this restriction does not apply in the event of an emergency. As for the proviso in the preceding Paragraph, the authority overseeing national intelligence should inform the dedicated judge of the high court concerned of the issuance of interception warrant and obtain the permission ex post facto. If permission is not granted within 48 hours, the surveillance activity should be halted.

Article 8

The foreign forces or the hostile foreign forces as

referred to in Paragraph 1
of the preceding Article are
defined as follows:

1. Foreign governments,
foreign or overseas political
entities, their subordinate
organizations or
representative agencies.

2. Organizations under the
direction or control of
foreign governments,
foreign or overseas political
entities.

3. Organizations with the
aim of operating
international or
cross-border terrorist
activities.

Article 9

An agent of foreign forces

or offshore hostile forces as

referred to in Article 7,

Paragraph 1 is defined as

follows:

1. A person who

participates, coerces

others, or abets others in

gathering secret

intelligence, or other secret

intelligence activities for

foreign forces or offshore

hostile forces, that risk

endangering national

security.

2. A person who

participates, coerces

others, or abets others in

sabotage or cross-border

terrorist activities for
foreign forces or offshore
hostile forces.

3. A person who serves as
an official, or an employee
for foreign forces or
offshore hostile forces, or
as a member of an
international terrorist
organization.

Article 10 Information gathered via
communication
surveillance pursuant to the
provisions of Article 7 is to
be used for national
security warning
intelligence purposes only.
However, if circumstances

as described in Article 5
are found, the information
obtained should be
forwarded to judicial police
authorities, judicial
authorities, or military
courts to be processed in
accordance with the law.

Article 11

The following information
should be included in an
interception warrant:

1. Grounds for the case,
and the laws and
regulations referencing the
alleged violation.
2. Surveillance subjects.
3. Features of the
communication

surveillance, such as types
or numbers, that is
sufficient for identification
purposes.

4. Surveillance location

5. Reasons for surveillance

6. Duration and methods

for surveillance

7. Petition agency

8. Enforcement agency

9. Setup organization

The enforcement agency

as referred to in

Subparagraph 8 of the

preceding Paragraph is the

agency involved in

gathering communication

contents. While the setup

organization as referred to

in Subparagraph 9 is the
organization that simply
provides the
software/hardware
components of
communication
surveillance equipment and
has no contact with
communication contents.
The procedure for issuing
an interception warrant
shall not be made public.

Article 11-1 When a prosecutor
investigates an offense
punishable by term
imprisonment of more than
3 years, if there are facts
leading to the belief that

communications records
and information of the
communications user are
necessary and relevant to
the investigation of the
case, unless in the situation
of an emergency for which
prior application is not
possible, a written
application should be filed
with the court for an access
warrant. For the matters to
be specified in the
application, Paragraph 1 of
the previous Article shall
apply mutatis mutandis.
When a judicial police
officer investigates the
situation of offense by a

criminal suspect and
collects evidence, if the
officer deems it necessary
to access the
communications records,
following the approval by
the prosecutor, an
application may be filed
with the court of jurisdiction
for issuance of an access
warrant in accordance with
the previous Paragraph.

When a prosecutor or
judicial police officer
investigates an offense
punishable by a term of
imprisonment of at least 10
years, the offense of
robbery, forcible taking,

fraud, extortion, kidnapping
for ransom or violation of
the Human Trafficking
Prevention Act, Statute for
Fire Arms, Ammunition and
Harmful Knives Control,
Statute for Punishment of
Smuggling, Narcotics
Hazard Prevention Act or
Organized Crime
Prevention Act, and if the
prosecutor or judicial police
officer deems it necessary,
the prosecutor may access
the communications record
ex officio, or the judicial
police officer may do so
after filing a request for
consent to the prosecutor,

and the restrictions under

the previous two

Paragraphs shall not apply.

After the reason of

emergency under

Paragraph 1 disappears,

an application should be

filed with the court for

issuance of an access

warrant.

The access warrant shall

specify the following:

1. The case.

2. The communications

records or user's

information to be accessed.

3. The validity period and

the specification that no

access shall be allowed

after expiration of said
period and that the access
warrant shall be returned
after access is obtained.

The court's decision to
reject any application under
Paragraphs 1, 2 or 4 shall
not be challenged.

The procedure for issuance
of an access warrant shall
not be public.

In case of any need to
access the
communications records of
any target of surveillance
under Article 7 and the
communications user's
information, the authority
overseeing national

intelligence may seek
access with the
telecommunications or
postal organization and the
restrictions under the
previous 7 Paragraphs
shall not apply.

Article 12 The communication
surveillance duration of
Articles 5 and Article 6 is
not to exceed 30 days each
time; while the
communication
surveillance duration of
Article 7 is not to exceed
one year each time. If it is
necessary to continue the
surveillance, specific

reasons must be specified,
and the last date for
petition should be no later
than two days before the
expiration date. However,
the period of continuous
surveillance under Articles
5 and 6 shall not exceed
one year. If the
enforcement authority
deems it necessary to
continue surveillance, a
new application shall be
filed in accordance with
Articles 5 and 6.

Prior to the expiration of the
communication
surveillance described in
Article 5 and Article 6, if the

surveillance is deemed as unnecessary by the prosecutor or the trial judge, the surveillance activity should be halted immediately.

Prior to the expiration of the communication surveillance described in Article 7, if the surveillance is deemed as unnecessary by the head of the authority overseeing national intelligence, the surveillance activity should be halted immediately.

Article 13

Surveillance should be conducted by intercepting,

wiretapping, sound
recording, video recording,
photographing, opening,
checking, copying
communications or other
similar necessary methods,
but there should be no
installation of listening
devices, video recording
equipment, or other
surveillance devices in a
private residence.

When implementing
communication
surveillance, with exception
to those having been dealt
with by the law, the
communications should be
maintained in a smooth and

open manner.

Unless the enforcement

authority has any

justification, the

surveillance recordings

should be collected every 3

days.

Any content of surveillance

recording under the

previous Paragraph that is

not related to the purpose

of surveillance shall not be

translated.

Article 14

The enforcement authority

and location for the

communication

surveillance should be

designated in accordance

with the request from the
petitioning agency. When a
judge issues an
interception warrant ex
officio, the issuer shall
designate such authority
and location; likewise,
when issuing a warrant
pursuant to the provisions
of Article 7.

Telecommunication
businesses and postal
services are obligated to
assist in the
implementation of
communication
surveillance. The items of
assistance include
providing communication

surveillance related

facilities for the use of the

enforcement authority, and

personnel assistance.

Expenses generated, while

assisting in the

implementation of

communication

surveillance as defined in

the preceding Paragraph,

may be reimbursed by the

enforcement authority after

the surveillance operation

is completed. The expense

items and fee standards

shall be formulated and

promulgated by the

Ministry of Transportation

and Communications in

consultation with relevant agencies.

The communication systems of telecommunication businesses should be equipped with the functions required to provide surveillance assistance.

While the telecommunication businesses are obligated to assist in the setup for the setup organization, and to maintain the communication surveillance system, its obligations are limited to having reasonable

technology and economic
development at the time of
setup, and expectations
should not exceed the
possibilities.

Expenses generated by
assisting in the setup of
communication
surveillance systems, as
defined in the preceding
Paragraph, shall be paid for
by the setup organization.

The necessary expenses
generated while assisting
in maintaining the normal
functions of the
communication
surveillance operation shall
be enacted and

promulgated by the
Ministry of Transportation
and Communications in
consultation with relevant
agencies.

Article 15 The enforcement authority
of communication
surveillance cases as
described in Article 5,
Article 6, and Article 7,
Paragraph 2 should, when
the communication
surveillance is over, state
the name, permanent
address or contact address
of the person under
surveillance, the
Subparagraph under Article

11, Paragraph 1 that is
applicable to the
surveillance case and
reference number of the
authority issuing the
interception warrant, the
actual period of
surveillance, whether
communications
information corresponding
to the purpose of the
surveillance has been
obtained and the remedy
procedure in the report to
the prosecutor, or the
authority overseeing
national intelligence, whom
in turn should report to the
court, so that the person

under surveillance may be notified. The report should also include the reasons if such a notification is deemed to be interfering with the purpose of the surveillance, or if the person should not be notified.

If the report under the previous Paragraph is not filed with the prosecutor and the authority overseeing national intelligence one month after the completion of the communications surveillance, the court shall notify the person under

surveillance within 14 days,
unless such notification is
not possible.

Upon receiving the report
as described in the first
Paragraph, the court
should notify the person
who was under
surveillance, with the
exception that if there is a
concrete reason showing
that such a notification is
deemed to be interfering
with the purpose of the
surveillance, or if the
person should not be
notified.

When the reasons for not
notifying cease to exist, the

enforcement authority
should submit a report to
the prosecutor, or the
authority overseeing
national intelligence, so
that the court may
supplement the notification.

If the reason has not
ceased to exist, the status
of said case shall be
continuously reported to
the court every three
months after submission of
the report under the
previous Paragraph. If the
report is not filed in time,
the court shall notify the
person under surveillance
within 14 days.

Contents of the report
submitted by the
enforcement authority shall
be verified by the court and
forwarded to the judicial
associate officer for use in
notifying the
communications service
user who was under
surveillance, except if such
a notification is not
possible.

The telecommunications
service users under
surveillance referred to in
the previous Paragraph
include individual,
institutions (agencies) or
organizations.

Article 16

Upon commencing the
communications
surveillance, the
enforcement authority
should submit a monthly
status report to the
prosecutor, the judge who
issued the interception
warrant or the head of the
authority overseeing
national intelligence. The
prosecutor, the judge who
issued the interception
warrant ex officio or the
head of the authority
overseeing national
intelligence may also
request that the
enforcement authority

submit reports at any time.

The supervision over a
communications
surveillance operation as
referred to in Article 5, or
Article 6 shall be assumed
by the prosecutorial agency
during the investigation, or
by the court during a trial.

The supervision over the
communications
surveillance operation as
referred to in Article 7 shall
be assumed by the
authority overseeing
national intelligence. The
authority will dispatch
personnel to the setup
organization or use

electronic supervision
devices, to supervise the
enforcement of the
communications
surveillance. For cases
under investigation, the
court shall dispatch
personnel to supervise the
enforcement authority on a
regular basis.

Article 16-1 The enforcement authority
and supervisory authority
for communications
surveillance shall prepare
an annual report with
relevant statistical
information of the
communications

surveillance performed
during the year. Said report
shall be published online
regularly and shall be
submitted to the Legislative
Yuan for reference.

The previous Paragraph
concerning regular online
publication shall not be
applicable to
communications
surveillance under Article
7.

The annual report of
statistical information under
Paragraph 1 shall include
the following matters:

1. Cases of applications
and approvals for

communications

surveillance under Articles

5, 6 and 7 and Article 12,

Paragraph 1, number of

targets under surveillance,

number of cases, number

of lines and types of lines.

The same shall be

applicable to case access

under Article 11-1.

2. Situations where

surveillance is stopped

under Article 12,

Paragraphs 2 and 3.

3. Notice or non-notice

under Article 15, types of

reasons for non-notice and

situations where the

reasons continue to or do

not continue to exist.

4. The court's supervision
of the enforcement by the
enforcement authority in
accordance with the
previous Article.

5. Execution of information
destruction in accordance
with Article 17.

6. Types and quantities of
intercepted records.

Article 17	The information obtained from the communication surveillance should be sealed or otherwise marked, and stamped by the enforcement authority to preserve its true
------------	--

completeness without
addition, deletion or
change. Information used
as case evidence shall be
kept in the file, or otherwise
kept for as long a time as is
necessary for surveillance
purposes. The enforcement
authority should safe-keep
the information for five
years after the
communication
surveillance is completed,
and destroy it afterwards.
For information obtained
from the communication
surveillance that is
completely irrelevant with
the surveillance objective,

the enforcement authority
should submit a report to
the prosecutor, the judge
who issued the interception
warrant ex officio or the
head of the authority
overseeing national
intelligence, and destroy
the information after
gaining their approval.

When destroying the
information as described in
the preceding two

Paragraphs, the
enforcement authority
should record the facts
concerning the
communication
surveillance, and submit a

request to the prosecutor,
the judge who issued the
interception warrant ex
officio or the head of the
authority overseeing
national intelligence to
dispatch an on-site
representative.

Article 18 Information obtained from
the communications
surveillance pursuant to
this Act shall not be
provided to other agencies
(institutions), groups or
individuals. However, this
restriction does not apply to
those complying with the
surveillance objective as

described in Article 5 or
Article 7, or other laws and
regulations.

Records of continuous
process flow shall be
established for the
safekeeping, use and
destruction of information
acquired from the
applications, issuances,
execution of interception
warrants under Articles 5
and 6. Network connection
shall be established with
the communications
surveillance management
system of the Taiwan High
Court.

The other authorities that

enforce communications
surveillance under the
previous Paragraph shall
transmit all interception
records to the
communications
surveillance management
system of the Taiwan High
Court through a designated
line or in a confidential
manner on a monthly basis.

Article 18-1 Any content about any
other case acquired
through communications
surveillance enforced in
accordance with Articles 5,
6 or 7 shall not be used as
evidence. However, a

submission may be filed
with the court within 7 days
from the discovery and
such evidence may be
admitted if the court
recognizes that said case is
related to the case for
which communications
surveillance is enforced or
if the case involves an
offense listed under any
Subparagraph under Article
5, Paragraph 1.

Any content acquired
through communications
surveillance enforced in
accordance with Articles 5,
6 or 7, or any evidence
deriving therefrom that is

not related to the purpose
of the surveillance, shall
not be used as evidence or
for any other purpose in
any judicial investigation,
judgment or other
proceeding and must be
destroyed in accordance
with Article 17, Paragraph
2.

Any content acquired
through interception that is
in violation of Articles 5, 6
or 7 or any evidence
deriving therefrom shall not
be used as evidence or
used for any other purpose
in any judicial investigation,
judgment or other

proceeding and must be
destroyed in accordance
with Article 17, Paragraph
2.

Article 19 Persons who conduct
communication
surveillance that violates
the provisions of this Act or
other laws, or leak, provide,
or use the information
obtained from such
communication
surveillance are liable for
damages.

Victims who suffered a
non-pecuniary damage
may claim a commensurate
amount of compensation;

those who suffered
damages to their reputation
may also request
appropriate punishment for
the restoration of their
reputation.

The right to claim as
described in the preceding
Paragraph shall not be
transferred or inherited.

However, this restriction
does not apply to those
claims where the
compensation amount has
been committed to in a
contract or where the
claims are in an ongoing
trial.

Article 20

The total compensation for the damage as described in the preceding Article shall be calculated based on the days of the communication surveillance: each person who was under surveillance may be compensated with more than one thousand and less than five thousand New Taiwan dollars per day. However, this restriction does not apply to those who can produce proof that the damage suffered is beyond this dollar amount.

If the total days of

communication
surveillance as described
in the preceding Paragraph
is unknown, the amount
shall be calculated as thirty
days.

Article 21 The right to claim begins
when the claimant realizes
the existence of a
damage-and-compensation
obligor, and ceases to exist
if the right is not exercised
in two years. Likewise,
when exceeding five years
since the damage
occurred.

Article 22 If civil servants or persons
entrusted with power of

authority, monitor others'
communications while
performing their duties, and
violate the provisions of this
Act or other laws, or leak,
provide, or use the
information obtained from
the communication
surveillance, then the
nation should bear the
responsibility for damage
compensation.

Provisions of Article 19
Paragraph 2, Paragraph 3,
and Article 20 are
applicable to the petitions
filed for national
compensation pursuant to
the provision of the

preceding Paragraph.

Article 23

Damage compensations

shall be determined in

accordance with the

provisions of this Act.

Provisions of the Civil Code

and the State

Compensation Law are

also applicable.

Article 24

Persons convicted of

illegally monitoring other

people's communications

are subject to a fixed-term

imprisonment of no more

than five years.

Civil servants or

employees, who enforce or

assist with the enforcement

of the communication
surveillance, thus
committing the offense as
described in the preceding
Paragraph by using the
power, opportunity or
means entrusted to their
duties or businesses are
subject to a fixed-term
imprisonment of more than
six months and less than
five years.

Those who commit the
offense as described in the
preceding two Paragraphs
with an intention of making
profits are subject to a
fixed-term imprisonment of
more than one year and

less than seven years.

Article 25

Persons who leak or give,

without good cause,

knowingly and illegally

obtained communication

surveillance information are

subject to a fixed-term

imprisonment of no more

than three years.

Persons who committed

the offense as described in

the preceding Paragraph

with an intention of making

profits are subject to a

fixed-term imprisonment of

more than six months and

less than five years.

Article 26

Information obtained via

illegally conducted

communication

surveillance as described

in the preceding two

Paragraphs will be

confiscated regardless of

whether or not it belongs to

the offender.

If the offender is unknown,

the confiscation shall be

pronounced independently.

Article 27

Civil servants or former civil

servants who have access

to secret information

because of the duties of

their positions or possess

such information obtained

via communications

surveillance conducted
pursuant to the provisions
of this Act or other laws,
leak or give away such
information without good
cause, are subject to a
fixed-term imprisonment of
no more than three years.

If any of the circumstances
set forth in Article 30,
Paragraph 2 or Article 89,
Paragraph 4 of the Judges
Act exists when a judge or
prosecutor applies this Act,
he or she shall be subject
to individual case
evaluation.

Civil servants or former civil
servant who use the

information acquired from
communications
surveillance in a case for
other purposes in violation
of Article 18-1, Paragraph 2
or 3 shall be subject to a
fixed-term imprisonment of
no more than three years.

Article 28

Non-civil servants, who are
aware of the secret
information due to their
duties or possess such
information obtained via
communication
surveillance conducted
pursuant to the provisions
of this Act or other laws,
and who leak or give away

such information without
good cause, are subject to
a fixed-term imprisonment
of no more than two years,
detention, or a fine of no
more than twenty thousand
New Taiwan dollars.

Article 29

If any one of the following
conditions is met when
conducting surveillance on
other people's
communications, it is not
punishable:

1. It is conducted pursuant
to the law.
 2. Employees of
telecommunication
businesses or postal
-

services organizations
(institutions) conducted the
surveillance based on the
objective of providing
public telecommunications
or postal services in
accordance with the
relevant laws.

3. The person conducting
the surveillance is one of
the parties in
communication, or has
obtained consent from one
of the parties in
communication, and the
conduct is not for illegal
purpose.

in Article 24, Paragraph 1;
Article 25, Paragraph 1,
and Article 28 are only
prosecutable upon
receiving a complaint.

Article 31 The telecommunication
businesses or postal
services organizations
(institutions) that are
obligated to assist in
enforcing communication
surveillance and have
violated the provisions of
Article 14, Paragraph 2
shall be subject to a fine of
more than five hundred
thousand and less than 2.5
million New Taiwan dollars

by the Ministry of
Transportation and
Communications. Those
who, upon receiving the
notification for compliance,
continue to violate the law
shall be fined continuously
on a daily basis, and their
special permits or permits
will be withdrawn.

Article 32 A military judicial authority,
during its investigation or
trial of active military
personnel concerning
communications
surveillance offenses, may
apply mutatis mutandis the
provisions of this Act.

Article 32-1

The Ministry of Justice shall
make annual reports to the
Legislative Yuan about the
status of the enforcement
of the communications
surveillance. If required,
the Legislative Yuan may
ask the Ministry of Justice
to make reports and may
ask to access relevant
information.

The Legislative Yuan may
send personnel at any time
to the infrastructure
authority,
telecommunications
enterprise, postal
enterprise or other
organizations, businesses

and premises that assist
with the enforcement of
communications
surveillance, to supervise
the status of enforcement
of communications
surveillance, or use
electronic monitoring
equipment to perform said
supervision.

Any matter that is not
provided in this Act shall be
exercised by the
Legislative Yuan ex officio
or subject to the application
of other laws.

Article 33

The enforcement rules of
this Act shall be formulated

by the Executive Yuan in
conjunction with the
Judicial Yuan.

Article 34 This Act is effective on the
date of promulgation.
The amended Articles shall
become effective five
months after the date of
promulgation.
