

ASSEMBLY BILL

No. 195

Introduced by Assembly Member Chau

January 28, 2015

An act to amend Sections 502 and 653f of the Penal Code, relating to computer crimes.

LEGISLATIVE COUNSEL'S DIGEST

AB 195, as introduced, Chau. Unauthorized access to computer systems.

(1) Existing law establishes various crimes related to computer services and systems. Existing law makes it a crime to knowingly, and without permission, access, cause to be accessed, or provide or assist in providing a means of accessing, a computer, computer system, computer network, or computer data in violation of prescribed provisions, and defines related terms.

This bill would specify that “computer network” for these purposes includes smartphones, as defined, and would make a conforming change.

(2) Existing law makes it a crime for a person, with the intent that the crime be committed, to solicit another to commit or join in the commission of prescribed crimes.

This bill would expand these provisions to make it a crime for a person, with the intent that the crime be committed, to solicit another to commit or join in the commission of the access crimes related to computer services and systems. The bill would make it a crime to offer to obtain or procure assistance for another to obtain unauthorized access, or to assist others in locating hacking services, as defined. The bill would make a violation of this provision punishable by imprisonment

in a county jail for a term not to exceed 6 months, or imprisonment for a term not to exceed one year for subsequent violations.

(3) By expanding the definitions of existing crimes, this bill would impose a state-mandated local program.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: yes.

The people of the State of California do enact as follows:

1 SECTION 1. Section 502 of the Penal Code is amended to
2 read:

3 502. (a) It is the intent of the Legislature in enacting this
4 section to expand the degree of protection afforded to individuals,
5 businesses, and governmental agencies from tampering,
6 interference, damage, and unauthorized access to lawfully created
7 computer data and computer systems. The Legislature finds and
8 declares that the proliferation of computer technology has resulted
9 in a concomitant proliferation of computer crime and other forms
10 of unauthorized access to computers, computer systems, and
11 computer data.

12 The Legislature further finds and declares that protection of the
13 integrity of all types and forms of lawfully created computers,
14 computer systems, and computer data is vital to the protection of
15 the privacy of individuals as well as to the well-being of financial
16 institutions, business concerns, governmental agencies, and others
17 within this state that lawfully utilize those computers, computer
18 systems, and data.

19 (b) For the purposes of this section, the following terms have
20 the following meanings:

21 (1) "Access" means to gain entry to, instruct, cause input to,
22 cause output from, cause data processing with, or communicate
23 with, the logical, arithmetical, or memory function resources of a
24 computer, computer system, or computer network.

25 (2) "Computer network" means any system that provides
26 communications between one or more computer systems and

1 input/output devices including, but not limited to, display terminals,
2 remote systems, mobile devices, *smartphones*, and printers
3 connected by telecommunication facilities.

4 (3) “Computer program or software” means a set of instructions
5 or statements, and related data, that when executed in actual or
6 modified form, cause a computer, computer system, or computer
7 network to perform specified functions.

8 (4) “Computer services” includes, but is not limited to, computer
9 time, data processing, or storage functions, Internet services,
10 electronic mail services, electronic message services, or other uses
11 of a computer, computer system, or computer network.

12 (5) “Computer system” means a device or collection of devices,
13 including support devices and excluding calculators that are not
14 programmable and capable of being used in conjunction with
15 external files, one or more of which contain computer programs,
16 electronic instructions, input data, and output data, that performs
17 functions including, but not limited to, logic, arithmetic, data
18 storage and retrieval, communication, and control.

19 (6) “Government computer system” means any computer system,
20 or part thereof, that is owned, operated, or used by any federal,
21 state, or local governmental entity.

22 (7) “Public safety infrastructure computer system” means any
23 computer system, or part thereof, that is necessary for the health
24 and safety of the public including computer systems owned,
25 operated, or used by drinking water and wastewater treatment
26 facilities, hospitals, emergency service providers,
27 telecommunication companies, and gas and electric utility
28 companies.

29 (8) “Data” means a representation of information, knowledge,
30 facts, concepts, computer software, computer programs or
31 instructions, *or smartphone applications*. Data may be in any form,
32 in storage media, or as stored in the memory of the computer or
33 in transit or presented on a display device.

34 (9) “Supporting documentation” includes, but is not limited to,
35 all information, in any form, pertaining to the design, construction,
36 classification, implementation, use, or modification of a computer,
37 computer system, computer network, computer program, or
38 computer software, which information is not generally available
39 to the public and is necessary for the operation of a computer,

1 computer system, computer network, computer program, or
2 computer software.

3 (10) “Injury” means any alteration, deletion, damage, or
4 destruction of a computer system, computer network, computer
5 program, or data caused by the access, or the denial of access to
6 legitimate users of a computer system, network, or program.

7 (11) “Victim expenditure” means any expenditure reasonably
8 and necessarily incurred by the owner or lessee to verify that a
9 computer system, computer network, computer program, or data
10 was or was not altered, deleted, damaged, or destroyed by the
11 access.

12 (12) “Computer contaminant” means any set of computer
13 instructions that are designed to modify, damage, destroy, record,
14 or transmit information within a computer, computer system, or
15 computer network without the intent or permission of the owner
16 of the information. They include, but are not limited to, a group
17 of computer instructions commonly called viruses or worms, that
18 are self-replicating or self-propagating and are designed to
19 contaminate other computer programs or computer data, consume
20 computer resources, modify, destroy, record, or transmit data, or
21 in some other fashion usurp the normal operation of the computer,
22 computer system, or computer network.

23 (13) “Internet domain name” means a globally unique,
24 hierarchical reference to an Internet host or service, assigned
25 through centralized Internet naming authorities, comprising a series
26 of character strings separated by periods, with the rightmost
27 character string specifying the top of the hierarchy.

28 (14) “Electronic mail” means an electronic message or computer
29 file that is transmitted between two or more telecommunications
30 devices; computers; computer networks, regardless of whether the
31 network is a local, regional, or global network; or electronic devices
32 capable or receiving electronic messages, regardless of whether
33 the message is converted to hard copy format after receipt, viewed
34 upon transmission, or stored for later retrieval.

35 (15) “Profile” means either of the following:

36 (A) A configuration of user data required by a computer so that
37 the user may access programs or services and have the desired
38 functionality on that computer.

39 (B) An Internet Web site user’s personal page or section of a
40 page that is made up of data, in text of graphical form, that displays

1 significant, unique, or identifying information, including, but not
2 limited to, listing acquaintances, interests, associations, activities,
3 or personal statements.

4 (16) “*Smartphone*” means a cellular radio telephone or other
5 mobile communications device that performs many of the functions
6 of a computer, typically having a touchscreen interface, Internet
7 access, and an operating system capable of running downloaded
8 applications.

9 (c) Except as provided in subdivision (h), any person who
10 commits any of the following acts is guilty of a public offense:

11 (1) Knowingly accesses and without permission alters, damages,
12 deletes, destroys, or otherwise uses any data, computer, computer
13 system, or computer network in order to either (A) devise or
14 execute any scheme or artifice to defraud, deceive, or extort, or
15 (B) wrongfully control or obtain money, property, or data.

16 (2) Knowingly accesses and without permission takes, copies,
17 or makes use of any data from a computer, computer system, or
18 computer network, or takes or copies any supporting
19 documentation, whether existing or residing internal or external
20 to a computer, computer system, or computer network.

21 (3) Knowingly and without permission uses or causes to be used
22 computer services.

23 (4) Knowingly accesses and without permission adds, alters,
24 damages, deletes, or destroys any data, computer software, or
25 computer programs which reside or exist internal or external to a
26 computer, computer system, or computer network.

27 (5) Knowingly and without permission disrupts or causes the
28 disruption of computer services or denies or causes the denial of
29 computer services to an authorized user of a computer, computer
30 system, or computer network.

31 (6) Knowingly and without permission provides or assists in
32 providing a means of accessing a computer, computer system, or
33 computer network in violation of this section.

34 (7) Knowingly and without permission accesses or causes to be
35 accessed any computer, computer system, or computer network.

36 (8) Knowingly introduces any computer contaminant into any
37 computer, computer system, or computer network.

38 (9) Knowingly and without permission uses the Internet domain
39 name or profile of another individual, corporation, or entity in
40 connection with the sending of one or more electronic mail

1 messages or posts and thereby damages or causes damage to a
2 computer, computer data, computer system, or computer network.

3 (10) Knowingly and without permission disrupts or causes the
4 disruption of government computer services or denies or causes
5 the denial of government computer services to an authorized user
6 of a government computer, computer system, or computer network.

7 (11) Knowingly accesses and without permission adds, alters,
8 damages, deletes, or destroys any data, computer software, or
9 computer programs which reside or exist internal or external to a
10 public safety infrastructure computer system computer, computer
11 system, or computer network.

12 (12) Knowingly and without permission disrupts or causes the
13 disruption of public safety infrastructure computer system computer
14 services or denies or causes the denial of computer services to an
15 authorized user of a public safety infrastructure computer system
16 computer, computer system, or computer network.

17 (13) Knowingly and without permission provides or assists in
18 providing a means of accessing a computer, computer system, or
19 public safety infrastructure computer system computer, computer
20 system, or computer network in violation of this section.

21 (14) Knowingly introduces any computer contaminant into any
22 public safety infrastructure computer system computer, computer
23 system, or computer network.

24 (d) (1) Any person who violates any of the provisions of
25 paragraph (1), (2), (4), (5), (10), (11), or (12) of subdivision (c) is
26 punishable by a fine not exceeding ten thousand dollars (\$10,000),
27 or by imprisonment pursuant to subdivision (h) of Section 1170
28 for 16 months, or two or three years, or by both that fine and
29 imprisonment, or by a fine not exceeding five thousand dollars
30 (\$5,000), or by imprisonment in a county jail not exceeding one
31 year, or by both that fine and imprisonment.

32 (2) Any person who violates paragraph (3) of subdivision (c)
33 is punishable as follows:

34 (A) For the first violation that does not result in injury, and
35 where the value of the computer services used does not exceed
36 nine hundred fifty dollars (\$950), by a fine not exceeding five
37 thousand dollars (\$5,000), or by imprisonment in a county jail not
38 exceeding one year, or by both that fine and imprisonment.

39 (B) For any violation that results in a victim expenditure in an
40 amount greater than five thousand dollars (\$5,000) or in an injury,

1 or if the value of the computer services used exceeds nine hundred
2 fifty dollars (\$950), or for any second or subsequent violation, by
3 a fine not exceeding ten thousand dollars (\$10,000), or by
4 imprisonment pursuant to subdivision (h) of Section 1170 for 16
5 months, or two or three years, or by both that fine and
6 imprisonment, or by a fine not exceeding five thousand dollars
7 (\$5,000), or by imprisonment in a county jail not exceeding one
8 year, or by both that fine and imprisonment.

9 (3) Any person who violates paragraph (6), (7), or (13) of
10 subdivision (c) is punishable as follows:

11 (A) For a first violation that does not result in injury, an
12 infraction punishable by a fine not exceeding one thousand dollars
13 (\$1,000).

14 (B) For any violation that results in a victim expenditure in an
15 amount not greater than five thousand dollars (\$5,000), or for a
16 second or subsequent violation, by a fine not exceeding five
17 thousand dollars (\$5,000), or by imprisonment in a county jail not
18 exceeding one year, or by both that fine and imprisonment.

19 (C) For any violation that results in a victim expenditure in an
20 amount greater than five thousand dollars (\$5,000), by a fine not
21 exceeding ten thousand dollars (\$10,000), or by imprisonment
22 pursuant to subdivision (h) of Section 1170 for 16 months, or two
23 or three years, or by both that fine and imprisonment, or by a fine
24 not exceeding five thousand dollars (\$5,000), or by imprisonment
25 in a county jail not exceeding one year, or by both that fine and
26 imprisonment.

27 (4) Any person who violates paragraph (8) or (14) of subdivision
28 (c) is punishable as follows:

29 (A) For a first violation that does not result in injury, a
30 misdemeanor punishable by a fine not exceeding five thousand
31 dollars (\$5,000), or by imprisonment in a county jail not exceeding
32 one year, or by both that fine and imprisonment.

33 (B) For any violation that results in injury, or for a second or
34 subsequent violation, by a fine not exceeding ten thousand dollars
35 (\$10,000), or by imprisonment in a county jail not exceeding one
36 year, or by imprisonment pursuant to subdivision (h) of Section
37 1170, or by both that fine and imprisonment.

38 (5) Any person who violates paragraph (9) of subdivision (c)
39 is punishable as follows:

1 (A) For a first violation that does not result in injury, an
2 infraction punishable by a fine not exceeding one thousand dollars
3 (\$1,000).

4 (B) For any violation that results in injury, or for a second or
5 subsequent violation, by a fine not exceeding five thousand dollars
6 (\$5,000), or by imprisonment in a county jail not exceeding one
7 year, or by both that fine and imprisonment.

8 (e) (1) In addition to any other civil remedy available, the owner
9 or lessee of the computer, computer system, computer network,
10 computer program, or data who suffers damage or loss by reason
11 of a violation of any of the provisions of subdivision (c) may bring
12 a civil action against the violator for compensatory damages and
13 injunctive relief or other equitable relief. Compensatory damages
14 shall include any expenditure reasonably and necessarily incurred
15 by the owner or lessee to verify that a computer system, computer
16 network, computer program, or data was or was not altered,
17 damaged, or deleted by the access. For the purposes of actions
18 authorized by this subdivision, the conduct of an unemancipated
19 minor shall be imputed to the parent or legal guardian having
20 control or custody of the minor, pursuant to the provisions of
21 Section 1714.1 of the Civil Code.

22 (2) In any action brought pursuant to this subdivision the court
23 may award reasonable attorney's fees.

24 (3) A community college, state university, or academic
25 institution accredited in this state is required to include
26 computer-related crimes as a specific violation of college or
27 university student conduct policies and regulations that may subject
28 a student to disciplinary sanctions up to and including dismissal
29 from the academic institution. This paragraph shall not apply to
30 the University of California unless the Board of Regents adopts a
31 resolution to that effect.

32 (4) In any action brought pursuant to this subdivision for a
33 willful violation of the provisions of subdivision (c), where it is
34 proved by clear and convincing evidence that a defendant has been
35 guilty of oppression, fraud, or malice as defined in subdivision (c)
36 of Section 3294 of the Civil Code, the court may additionally award
37 punitive or exemplary damages.

38 (5) No action may be brought pursuant to this subdivision unless
39 it is initiated within three years of the date of the act complained
40 of, or the date of the discovery of the damage, whichever is later.

1 (f) This section shall not be construed to preclude the
2 applicability of any other provision of the criminal law of this state
3 which applies or may apply to any transaction, nor shall it make
4 illegal any employee labor relations activities that are within the
5 scope and protection of state or federal labor laws.

6 (g) Any computer, computer system, computer network, or any
7 software or data, owned by the defendant, that is used during the
8 commission of any public offense described in subdivision (c) or
9 any computer, owned by the defendant, which is used as a
10 repository for the storage of software or data illegally obtained in
11 violation of subdivision (c) shall be subject to forfeiture, as
12 specified in Section 502.01.

13 (h) (1) Subdivision (c) does not apply to punish any acts which
14 are committed by a person within the scope of his or her lawful
15 employment. For purposes of this section, a person acts within the
16 scope of his or her employment when he or she performs acts
17 which are reasonably necessary to the performance of his or her
18 work assignment.

19 (2) Paragraph (3) of subdivision (c) does not apply to penalize
20 any acts committed by a person acting outside of his or her lawful
21 employment, provided that the employee's activities do not cause
22 an injury, to the employer or another, or provided that the value
23 of supplies or computer services which are used does not exceed
24 an accumulated total of two hundred fifty dollars (\$250).

25 (i) No activity exempted from prosecution under paragraph (2)
26 of subdivision (h) which incidentally violates paragraph (2), (4),
27 or (7) of subdivision (c) shall be prosecuted under those paragraphs.

28 (j) For purposes of bringing a civil or a criminal action under
29 this section, a person who causes, by any means, the access of a
30 computer, computer system, or computer network in one
31 jurisdiction from another jurisdiction is deemed to have personally
32 accessed the computer, computer system, or computer network in
33 each jurisdiction.

34 (k) In determining the terms and conditions applicable to a
35 person convicted of a violation of this section the court shall
36 consider the following:

37 (1) The court shall consider prohibitions on access to and use
38 of computers.

39 (2) Except as otherwise required by law, the court shall consider
40 alternate sentencing, including community service, if the defendant

1 shows remorse and recognition of the wrongdoing, and an
2 inclination not to repeat the offense.

3 SEC. 2. Section 653f of the Penal Code is amended to read:

4 653f. (a) Every person who, with the intent that the crime be
5 committed, solicits another to offer, accept, or join in the offer or
6 acceptance of a bribe, or to commit or join in the commission of
7 carjacking, robbery, burglary, grand theft, receiving stolen property,
8 extortion, perjury, subornation of perjury, forgery, kidnapping,
9 arson or assault with a deadly weapon or instrument or by means
10 of force likely to produce great bodily injury, or, by the use of
11 force or a threat of force, to prevent or dissuade any person who
12 is or may become a witness from attending upon, or testifying at,
13 any trial, proceeding, or inquiry authorized by law, shall be
14 punished by imprisonment in a county jail for not more than one
15 year or pursuant to subdivision (h) of Section 1170, or by a fine
16 of not more than ten thousand dollars (\$10,000), or the amount
17 which could have been assessed for commission of the offense
18 itself, whichever is greater, or by both the fine and imprisonment.

19 (b) Every person who, with the intent that the crime be
20 committed, solicits another to commit or join in the commission
21 of murder shall be punished by imprisonment in the state prison
22 for three, six, or nine years.

23 (c) Every person who, with the intent that the crime be
24 committed, solicits another to commit rape by force or violence,
25 sodomy by force or violence, oral copulation by force or violence,
26 or any violation of Section 264.1, 288, or 289, shall be punished
27 by imprisonment in the state prison for two, three, or four years.

28 (d) (1) Every person who, with the intent that the crime be
29 committed, solicits another to commit an offense specified in
30 Section 11352, 11379, 11379.5, 11379.6, or 11391 of the Health
31 and Safety Code shall be punished by imprisonment in a county
32 jail not exceeding six months. Every person, who, having been
33 convicted of soliciting another to commit an offense specified in
34 this subdivision, is subsequently convicted of the proscribed
35 solicitation, shall be punished by imprisonment in a county jail
36 not exceeding one year, or pursuant to subdivision (h) of Section
37 1170.

38 (2) This subdivision does not apply where the term of
39 imprisonment imposed under other provisions of law would result
40 in a longer term of imprisonment.

1 (e) Every person who, with the intent that the crime be
 2 committed, solicits another to commit an offense specified in
 3 Section 14014 of the Welfare and Institutions Code shall be
 4 punished by imprisonment in a county jail for not exceeding six
 5 months. Every person who, having been convicted of soliciting
 6 another to commit an offense specified in this subdivision, is
 7 subsequently convicted of the proscribed solicitation, shall be
 8 punished by imprisonment in a county jail not exceeding one year,
 9 or pursuant to subdivision (h) of Section 1170.

10 (f) (1) *Every person who, with the intent that the crime be*
 11 *committed, solicits another to commit an offense set forth in Section*
 12 *502 shall be punished as set forth in paragraph (3).*

13 (2) *Every person who, with the intent that the crime be*
 14 *committed, offers to solicit assistance for another to conduct*
 15 *activities in violation of Section 502 shall be punished as set forth*
 16 *in paragraph (3). This includes persons operating Internet Web*
 17 *sites that offer to assist others in locating hacking services. For*
 18 *the purposes of this section “hacking services” means assistance*
 19 *in the unauthorized access to computers, computer systems, or*
 20 *computer data in violation of Section 502.*

21 (3) *Every person who violates this subdivision shall be punished*
 22 *by imprisonment in a county jail for a period not to exceed six*
 23 *months. Every subsequent violation of this subdivision by that*
 24 *same person shall be punished by imprisonment in a county jail*
 25 *not exceeding one year, or pursuant to subdivision (h) of Section*
 26 *1170.*

27 (f)

28 (g) An offense charged in violation of subdivision (a), (b), or
 29 (c) shall be proven by the testimony of two witnesses, or of one
 30 witness and corroborating circumstances. An offense charged in
 31 violation of subdivision ~~(d) or (e)~~ (d), (e), or (f) shall be proven
 32 by the testimony of one witness and corroborating circumstances.

33 SEC. 3. No reimbursement is required by this act pursuant to
 34 Section 6 of Article XIII B of the California Constitution because
 35 the only costs that may be incurred by a local agency or school
 36 district will be incurred because this act creates a new crime or
 37 infraction, eliminates a crime or infraction, or changes the penalty
 38 for a crime or infraction, within the meaning of Section 17556 of
 39 the Government Code, or changes the definition of a crime within

- 1 the meaning of Section 6 of Article XIII B of the California
- 2 Constitution.

O