<proposed revision: draft; Hal Berghel; February 6, 2014>

UNLAWFUL ACTS REGARDING COMPUTERS AND INFORMATION SERVICES

NRS 205.473 Definitions. As used in NRS 205.473 to 205.513, inclusive, unless the context otherwise requires, the words and terms defined in NRS 205.4732 to 205.476, inclusive, have the meanings ascribed to them in those sections.

(Added to NRS by 1983, 1203; A 1991, 50; 1999, 2707; 2001, 1240)

NRS 205.4732 "Unauthorized Access" defined. "Unauthorized Access" ~~means to intercept, instruct, communicate with, store data in, retrieve from or otherwise make use of any resources of a computer, network or data.~~ to a computer, its equipment, or any data therein, means knowingly, intentionally, and invasively overcoming security measures to gain entry to a system or access to data therein which one does not own or does not have the expressed or implied permission of the owner to access.

1. The term does not include accessing publicly available computers or web servers or any publicly available data therein. It is incumbent upon publishers of data and owners of computers to implement security measures when and where it is desired.

2. The term does not in any way include the inspection, modification, or tampering with personal property by the owner of said property

(Added to NRS by 1991, 49)

NRS 205.4733 "Digital Storage" defined. "Digital storage" means the retention of data by for the purpose of subsequent use by a computer or network resource. "Ephemeral storage" means the retention of data for a short time that is required by the normal operation of a program or service where the data is no longer accessible by the host operating system after the execution of the program or service ends.

NRS 205.4734 "Industry best-practices" defined. "Industry best-practices" with respect to cryptography and digital security, means the intersection of behaviors and protocols widely believed to be currently sufficient to cryptographically safeguard data from unauthorized parties.

NRS 205.4735 "Computer" defined. "Computer" means an electronic device which performs or is capable of performing logical, arithmetic and memory functions by manipulations of ~~electronic or magnetic~~digital ~~impulses and includes all equipment related to the computer in a system or network.~~ signals, including, without limitation, computers in any form or size, including but not limited to personal digital assistants, routers, switches, cell phones, embedded devices, digital cameras, gaming consoles, printers, DVD and Blueray players, CD players, mp3 players, digital video recorders, and anything else capable of electronically processing digital data.

(Added to NRS by 1983, 1203)

NRS 205.4736 "Computer equipment" defined. "Computer equipment" means any device ~~or program~~ used in the normal operation of a computer, including, without limitation, peripheral devices such as mice and keyboards, external and internal storage devices, audio and video devices, printers, and networking equipment such as routers, switches, cables, modems, and antennae.

NRS 205.4737 "Computer contaminant" defined.

~~1.~~ "Computer contaminant" means any data, information, image, program, signal ~~or sound that is designed or has the capability to:~~, sound, or device that has the capability to corrupt, disrupt, damage, destroy, or modify a computer or its equipment, or to corrupt, disrupt, damage, destroy, modify, record, or transmit any data therein without the expressed knowledge and consent of the owner of the computer or computer equipment.

1. The term includes, without limitation: any computer virus, worm, Trojan horse, rootkit, malware, ransomware, adware, spyware, browser extension or control, or exploit, that operates~~,~~ without the expressed knowledge and consent of the owner of a computer and its equipment:

(a) Tracks, records, or transmits computer activity or data, including, without limitation, user activity, audio data, video data, web searches, keystrokes, RF signals, environmental measurements, or location data; or

(b) Has the capability to prevent, impede, delay, or otherwise disrupt or compromise the security, integrity, or normal operation of a computer or its equipment.

2. The term does not include any program, data, or device that exists or persists on a computer or its equipment with the knowledge and consent of the owner.

~~(a) Contaminate, corrupt, consume, damage, destroy, disrupt, modify, record or transmit; or~~

~~(b) Cause to be contaminated, corrupted, consumed, damaged, destroyed, disrupted, modified, recorded or transmitted,~~

~~ any other data, information, image, program, signal or sound contained in a computer, system or network without the knowledge or consent of the person who owns the other data, information, image, program, signal or sound or the computer, system or network.~~

~~2. The term includes, without limitation:~~

~~(a) A virus, worm or Trojan horse;~~

~~(b) Spyware that tracks computer activity and is capable of recording and transmitting such information to third parties; or~~

~~(c) Any other similar data, information, image, program, signal or sound that is designed or has the capability to prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system or network.~~

~~3. As used in this section:~~

~~(a) "On-line bidding" has the meaning ascribed to it in NRS 332.047.~~

~~(b) "Spyware" does not include:~~

~~(1) An Internet browser;~~

~~(2) Software for transmitting messages instantly that informs the user whether other users are on-line at the same time;~~

~~(3) Software that is designed to detect or prevent the use of computer contaminants;~~

~~(4) Software that is designed to detect fraudulent on-line bidding;~~

~~(5) Software that is designed to prevent children from accessing pornography on the Internet;~~

~~(6) Software that conducts remote maintenance or repair of a computer or its systems;~~

~~(7) Software that is designed to manage or to perform maintenance on a network of computers;~~

~~(8) Software for media players; and~~

~~(9) Software that authenticates a user.~~

(Added to NRS by 1999, 2703; A 2005, 2509; 2005, 22nd Special Session, 97)

NRS 205.4738 "Network forgery" defined. "Network forgery" means the intentional and disruptive redirection, interception, or modification of network traffic by means of modifying or substituting any routing or addressing information used to direct packets or data around a network, or of any means of authenticating said packets or data between communicating parties.

1. The term includes, without limitation, IP spoofing, ARP spoofing, DNS spoofing, DNS cache poisoning, SSL/TLS stripping and spoofing, and any man-in-the-middle, redirection, or replay attacks.

NRS 205.4739 "Unlawful tampering" defined. "Unlawful tampering" with respect to computers, computer equipment, and data means any intentional and invasive act which, without authorization, results in network forgery or the introduction of a computer contaminant to a computer or computer equipment, as defined.

1. The term does not include tampering with one's own property or with computers or computer equipment for which one has an express, implied, or contractual right to do so.

NRS 205.474 "Data" defined. "Data" means a representation in ~~any~~ digital form of information, knowledge, facts, concepts or instructions prepared for use by a computer or computer equipment.~~which is being prepared or has been formally prepared and is intended to be processed, is being processed or has been processed in a system or network.~~

(Added to NRS by 1983, 1203)

NRS 205.4741 "User data" defined. "User data" means any data about or concerning users of an information service.

NRS 205.4742 "Encryption" ,"Steganography" and "Covert Channeling" defined. "Encryption" means the use of any ~~protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding or a computer contaminant, to:~~ cryptographic mechanism(s) to protect data by obscuring its real meaning to unauthorized parties. "Steganography" means the hiding of data within other data in such a way as to make it undetectable through the normal use of computing equipment to anyone other than the sender and intended recipient. "Covert Channeling" means the hiding of data within computer programs, computer systems, or computer networks, by using techniques that are not intended for that type of communication.

~~1. Prevent, impede, delay or disrupt access to any data, information, image, program, signal or sound;~~

~~2. Cause or make any data, information, image, program, signal or sound unintelligible or unusable; or~~

~~3. Prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system or network.~~

(Added to NRS by 1999, 2704)

NRS 205.4743 "Information service" defined.

~~1.~~ "Information service" means a service that is designed or has the capability to generate, process, store, retrieve, convey, emit, transmit, receive, relay, record or reproduce any data~~,~~

~~information, image, program, signal or sound by means of any component, device, equipment, system or network, including, without limitation, by means of~~

1. The term does not include computers or networks of computers for personal or non-organizational use.

~~(a) A computer, computer system, computer network, modem or scanner.~~

~~(b) A telephone, cellular phone, satellite phone, pager, personal communications device or facsimile machine.~~

~~(c) Any type of transmitter or receiver.~~

~~(d) Any other component, device, equipment, system or network that uses analog, digital, electronic, electromagnetic, magnetic or optical technology.~~

~~2. The term does not include video service, as defined in NRS 711.141.~~

(Added to NRS by 1999, 2704; A 2007, 1377)

NRS 205.4744 "Internet or network site" defined.

1. "Internet or network site" means any identifiable site on the Internet or on a network.

2. The term includes, without limitation:

(a) A website or other similar site on the World Wide Web;

(b) A site that is identifiable through a Uniform Resource Location;

(c) A site on a network that is owned, operated, administered or controlled by a provider of Internet service;

(d) An electronic bulletin board;

(e) A list server;

(f) A newsgroup; or

(g) A chat room.

(Added to NRS by 2001, 1240)

NRS 205.4745 "Network" defined. "Network" means a set of related, remotely connected devices and facilities, including more than one system, with the capability to transmit

data among any of the devices and facilities. The term includes, without limitation, a local, regional or global computer network.

(Added to NRS by 1983, 1203; A 1999, 2707)

NRS 205.4746 "Hashing" defined. "Hashing" means the processing of data using cryptographic hash algorithms.

NRS 205.4747 "Plaintext" defined. "Plaintext" means any data unprotected by encryption, as defined.

NRS 205.4748 "Data identifier" defined. "Data identifier" means any part of data which carries plaintext meaning about the source or destination of itself or other data, including, without limitation, IP addresses, MAC addresses, phone numbers, physical addresses, user names, host names, or any other information capable of uniquely or somewhat uniquely identifying a person(s) or organization.

NRS 205.4749 "Anonymization" defined. "Anonymization" with respect to user data digitally stored by information services means hashing its identifiers at least twice and not retaining any original copies, as defined.

NRS 205.475 "Program" defined. "Program" means an ordered set of data representing coded instructions or statements which can be executed by a computer and cause the computer to perform one or more tasks.

(Added to NRS by 1983, 1203)

NRS 205.4751 "Communications data" defined. "Communications data" means the content of digital communications, including, without limitation, the content of email, text messages, audio and/or video transmissions, instant messages, and Internet relay chat.

1. The term does not include communications that are public in nature, such as blog, forum, and social media posts that were publicly accessible when they were created and were publicly accessible thereafter.

NRS 205.4734 "Expressed knowledge and consent" defined. "Expressed knowledge and consent" means formally accepting an end-user agreement, privacy policy, or contract, as confirmed by click-through or digital signature, which clearly describes the forfeiture of one's default rights as described in this section.

NRS 205.4755 "Property" defined. "Property" means anything of value and includes a financial instrument, information, electronically produced data, program and any other tangible or intangible item of value.

(Added to NRS by 1983, 1203)

NRS 205.4757 "Provider" defined. "Provider" means any person who provides an information service.

(Added to NRS by 1999, 2704)

NRS 205.4758 "Provider of Internet service" defined. "Provider of Internet service" means any provider who provides subscribers with access to the Internet or an electronic mail address, or both.

(Added to NRS by 1999, 2704)

NRS 205.4759 "Response costs" defined.

1. "Response costs" means any reasonable costs that arise in response to and as a proximate result of a crime described in NRS 205.473 to 205.513, inclusive.

2. The term includes, without limitation, any reasonable costs to:

(a) Investigate the facts surrounding the crime;

(b) Ascertain or calculate any past or future loss, injury or other damage;

(c) Remedy, mitigate or prevent any past or future loss, injury or other damage; or

(d) Test, examine, restore or verify the integrity of or the normal operation or use of any Internet or network site, electronic mail address, computer, system, network, component, device, equipment, data, information, image, program, signal or sound.

(Added to NRS by 2001, 1240)

NRS 205.476 "System" defined. "System" means a set of related equipment, whether or not connected, which is used with or for a computer.

(Added to NRS by 1983, 1203)

~~NRS 205.4765 Unlawful acts regarding computers: Generally.~~

~~1. Except as otherwise provided in subsection 6, a person who knowingly, willfully and without authorization:~~

~~(a) Modifies;~~

~~(b) Damages;~~

~~(c) Destroys;~~

~~(d) Discloses;~~

~~(e) Uses;~~

~~(f) Transfers;~~

~~(g) Conceals;~~

~~(h) Takes;~~

~~(i) Retains possession of;~~

~~(j) Copies;~~

~~(k) Obtains or attempts to obtain access to, permits access to or causes to be accessed; or~~

~~(l) Enters,~~

~~ data, a program or any supporting documents which exist inside or outside a computer, system or network is guilty of a misdemeanor.~~

~~2. Except as otherwise provided in subsection 6, a person who knowingly, willfully and without authorization:~~

~~(a) Modifies;~~

~~(b) Destroys;~~

~~(c) Uses;~~

~~(d) Takes;~~

~~(e) Damages;~~

~~(f) Transfers;~~

~~(g) Conceals;~~

~~(h) Copies;~~

~~(i) Retains possession of; or~~

~~(j) Obtains or attempts to obtain access to, permits access to or causes to be accessed,~~

~~ equipment or supplies that are used or intended to be used in a computer, system or network is guilty of a misdemeanor.~~

~~3. Except as otherwise provided in subsection 6, a person who knowingly, willfully and without authorization:~~

~~(a) Destroys;~~

~~(b) Damages;~~

~~(c) Takes;~~

~~(d) Alters;~~

~~(e) Transfers;~~

~~(f) Discloses;~~

~~(g) Conceals;~~

~~(h) Copies;~~

~~(i) Uses;~~

~~(j) Retains possession of; or~~

~~(k) Obtains or attempts to obtain access to, permits access to or causes to be accessed,~~

~~ a computer, system or network is guilty of a misdemeanor.~~

~~4. Except as otherwise provided in subsection 6, a person who knowingly, willfully and without authorization:~~

~~(a) Obtains and discloses;~~

~~(b) Publishes;~~

~~(c) Transfers; or~~

~~(d) Uses,~~

~~ a device used to access a computer, network or data is guilty of a misdemeanor.~~

~~5. Except as otherwise provided in subsection 6, a person who knowingly, willfully and without authorization introduces, causes to be introduced or attempts to introduce a computer contaminant into a computer, system or network is guilty of a misdemeanor.~~

~~6. If the violation of any provision of this section:~~

(a) Was committed to devise or execute a scheme to defraud or illegally obtain property;

(b) Caused response costs, loss, injury or other damage in excess of $500; or

(c) Caused an interruption or impairment of a public service, including, without limitation, a governmental operation, a system of public communication or transportation or a supply of water, gas or electricity,

 the person is guilty of a category C felony and shall be punished as provided in NRS 193.130, and may be further punished by a fine of not more than $100,000. In addition to any other penalty, the court shall order the person to pay restitution.

7. The provisions of this section do not apply to a person performing any testing, including, without limitation, penetration testing, of an information system of an agency that uses the equipment or services of the Division of Enterprise Information Technology Services that is authorized by the Administrator of the Division of Enterprise Information Technology Services or the head of the Office of Information Security of the Division. As used in this subsection:

(a) "Information system" has the meaning ascribed to it in NRS 242.057.

(b) "Penetration testing" has the meaning ascribed to it in NRS 242.171.

(Added to NRS by 1983, 1203; A 1991, 50; 1995, 1228; 1999, 2707; 2001, 1240; 2011, 1862)

NRS 205.477 Unlawful interference with or denial of access to or use of computers; unlawful use or access of computers; affirmative defense.

1. Except as otherwise provided in subsections 3 and 4, a person who knowingly, willfully, maliciously and without authorization interferes with, denies or causes the denial of access to or use of a computer, system or network to a person who has the duty and right to use it is guilty of a gross misdemeanor.

2. Except as otherwise provided in subsections 3 and 4, a person who knowingly, willfully, maliciously and without authorization uses, causes the use of, accesses, attempts to gain access to or causes access to be gained to a computer, system, network, telecommunications device, telecommunications service or information service is guilty of a gross misdemeanor.

3. If the violation of any provision of this section:

(a) Was committed to devise or execute a scheme to defraud or illegally obtain property;

(b) Caused response costs, loss, injury or other damage in excess of $500; or

(c) Caused an interruption or impairment of a public service, including, without limitation, a governmental operation, a system of public communication or transportation or a supply of water, gas or electricity,

 the person is guilty of a category C felony and shall be punished as provided in NRS 193.130, and may be further punished by a fine of not more than $100,000. In addition to any other penalty, the court shall order the person to pay restitution.

4. It is an affirmative defense to a charge made pursuant to this section that at the time of the alleged offense the defendant reasonably believed that:

(a) The defendant was authorized to use or access the computer, system, network, telecommunications device, telecommunications service or information service and such use or access by the defendant was within the scope of that authorization; or

(b) The owner or other person authorized to give consent would authorize the defendant to use or access the computer, system, network, telecommunications device, telecommunications service or information service.

5. A defendant who intends to offer an affirmative defense described in subsection 4 at a trial or preliminary hearing must, not less than 14 days before the trial or hearing or at such other time as the court may direct, file and serve on the prosecuting attorney a written notice of that intent.

(Added to NRS by 1983, 1204; A 1991, 51; 1995, 1229; 1999, 2709; 2001, 1242; 2011, 3650)

NRS 205.481 Forgery by creation, alteration or deletion of data, information, image, program, signal or sound contained in computer. A person who knowingly, willfully and without authorization creates, alters or deletes any data, information, image, program, signal or sound contained in any computer, system or network which, if done on a written or printed document or instrument, would constitute forgery pursuant to NRS 205.090 or 205.095, is guilty of forgery which is a category D felony and shall be punished as provided in NRS 193.130.

(Added to NRS by 1991, 49; A 1995, 1229; 1999, 2709)

NRS 205.486 Unlawful use of encryption.

1. A person shall not willfully use or attempt to use encryption, directly or indirectly, to:

(a) Commit, facilitate, further or promote any criminal offense;

(b) Aid, assist or encourage another person to commit any criminal offense;

(c) Conceal the commission of any criminal offense;

(d) Conceal or protect the identity of a person who has committed any criminal offense; or

(e) Delay, hinder or obstruct the administration of the law.

2. A person who violates any provision of this section:

(a) Is guilty of a gross misdemeanor, unless the encryption was used or attempted to be used to commit a crime for which a greater penalty is provided by specific statute. If the encryption was used or attempted to be used to commit a crime for which a greater penalty is provided by specific statute, the person shall be punished as prescribed by statute for that crime.

(b) Commits a criminal offense that is separate and distinct from any other criminal offense and may be prosecuted and convicted pursuant to this section whether or not the person or any other person is or has been prosecuted or convicted for any other criminal offense arising out of the same facts as the violation of this section.

(Added to NRS by 1999, 2704; A 2001, 2789)

NRS 205.492 Unlawful acts involving electronic mail or transmission of other data, information, images, programs, signals or sounds to computer, system or network.

1. A person shall not willfully falsify or forge any data, information, image, program, signal or sound that:

(a) Is contained in the header, subject line or routing instructions of an item of electronic mail; or

(b) Describes or identifies the sender, source, point of origin or path of transmission of an item of electronic mail,

 with the intent to transmit or cause to be transmitted the item of electronic mail to any Internet or network site or to the electronic mail address of one or more recipients without their knowledge of or consent to the transmission.

2. Except as otherwise provided in subsection 7, a person shall not willfully transmit or cause to be transmitted an item of electronic mail to any Internet or network site or to the electronic mail address of one or more recipients without their knowledge of or consent to the transmission if the person knows or has reason to know that the item of electronic mail contains or has been generated or formatted with:

(a) An Internet domain name that is being used without the consent of the person who holds the Internet domain name; or

(b) Any data, information, image, program, signal or sound that has been used intentionally in the header, subject line or routing instructions of the item of electronic mail to falsify or misrepresent:

(1) The identity of the sender; or

(2) The source, point of origin or path of transmission of the item of electronic mail.

3. A person shall not knowingly sell, give or otherwise distribute or possess with the intent to sell, give or otherwise distribute any data, information, image, program, signal or sound which is designed or intended to be used to falsify or forge any data, information, image, program, signal or sound that:

(a) Is contained in the header, subject line or routing instructions of an item of electronic mail; or

(b) Describes or identifies the sender, source, point of origin or path of transmission of an item of electronic mail.

4. Except as otherwise provided in subsection 7, a person shall not willfully and without authorization transmit or cause to be transmitted an item of electronic mail or any other data, information, image, program, signal or sound to any Internet or network site, to the electronic mail address of one or more recipients or to any other computer, system or network:

(a) With the intent to prevent, impede, delay or disrupt the normal operation or use of the Internet or network site, electronic mail address, computer, system or network, whether or not such a result actually occurs; or

(b) Under circumstances in which such conduct is reasonably likely to prevent, impede, delay or disrupt the normal operation or use of the Internet or network site, electronic mail address, computer, system or network, whether or not such a result actually occurs.

5. Except as otherwise provided in subsection 6, a person who violates any provision of this section is guilty of a misdemeanor.

6. If the violation of any provision of subsection 4:

(a) Was committed to devise or execute a scheme to defraud or illegally obtain property;

(b) Caused response costs, loss, injury or other damage in excess of $500; or

(c) Caused an interruption or impairment of a public service, including, without limitation, a governmental operation, a system of public communication or transportation or a supply of water, gas or electricity,

 the person is guilty of a category C felony and shall be punished as provided in NRS 193.130, and may be further punished by a fine of not more than $100,000. In addition to any other penalty, the court shall order the person to pay restitution.

7. The provisions of subsections 2 and 4 do not apply to a provider of Internet service who, in the course of providing service, transmits or causes to be transmitted an item of electronic mail on behalf of another person, unless the provider of Internet service is the person who first generates the item of electronic mail.

8. As used in this section, "item of electronic mail" includes, without limitation:

(a) A single item of electronic mail;

(b) Multiple copies of one or more items of electronic mail;

(c) A collection, group or bulk aggregation of one or more items of electronic mail;

(d) A constant, continual or recurring pattern or series of one or more items of electronic mail; or

(e) Any other data, information, image, program, signal or sound that is included or embedded in or attached or connected to one or more items of electronic mail.

(Added to NRS by 1999, 2704; A 2001, 1243)

NRS 205.498 Provider of Internet service required to keep certain information concerning subscribers confidential; notice required to be provided to subscribers.

1. A provider of Internet service shall keep confidential:

(a) All information concerning a subscriber, other than the electronic mail address of the subscriber, unless the subscriber gives permission, in writing or by electronic mail, to the provider of Internet service to disclose the information.

(b) The electronic mail address of a subscriber, if the subscriber requests, in writing or by electronic mail, to have the electronic mail address of the subscriber kept confidential. Upon receiving such a request from a subscriber, a provider of Internet service shall keep confidential the electronic mail address of the subscriber, unless the subscriber gives permission, in writing or by electronic mail, to the provider of Internet service to disclose the electronic mail address of the subscriber.

2. A provider of Internet service shall provide notice of the requirements of subsection 1 to each of its subscribers. The notice must include, without limitation, a conspicuous statement that a subscriber may request, in writing or by electronic mail, to have the electronic mail address of the subscriber kept confidential.

3. A provider of Internet service who violates any provision of this section is guilty of a misdemeanor and shall be punished by a fine of not less than $50 or more than $500 for each violation.

4. As used in this section, "provider of Internet service" means a provider of Internet service who charges a subscriber for access to the Internet or the electronic mail address of the subscriber.

(Added to NRS by 1999, 2705)

NRS 205.506 Unlawful acts regarding information services.

1. It is unlawful for a person knowingly and with the intent to avoid payment in full for the service obtained to:

(a) Obtain or attempt to obtain an information service from a provider by deception, use of an illegal device or other fraudulent means. The requisite intent may be inferred from the presence on the property or in the possession of the person of a device, not authorized by the provider, the major purpose of which is to permit or facilitate use of an information service without payment. The inference is rebutted if the person shows that he or she purchased the device for a legitimate purpose.

(b) Give to another person technical assistance or instruction in obtaining an information service without full payment to a provider.

(c) Maintain an ability to connect, by physical, electronic or other means, with facilities, components or devices used in an information service for the purpose of obtaining the information service without payment of all lawful compensation to the provider.

(d) Make or maintain a modification of a device installed with the authorization of a provider to obtain any service that the person is not authorized by the provider to obtain. The requisite intent may be inferred from proof that the standard procedure of the provider is to place labels on its devices warning that modifying the device is a violation of law and that the device has been modified without the permission of the provider.

(e) Possess, manufacture, deliver, offer to deliver or advertise, without permission from the provider, a device or a kit for a device designed to:

(1) Receive from the provider a service offered for sale by the provider, whether or not the service is encoded or otherwise made unintelligible; or

(2) Perform or facilitate an act prohibited by paragraphs (a) to (d), inclusive.

 Intent to violate this paragraph for commercial advantage or financial gain may be inferred if the circumstances, including, without limitation, quantity or volume, indicate possession for resale.

(f) Manufacture, import, distribute, advertise, sell, lease, or offer to sell or lease a device or a plan or kit for a device designed to receive an information service offered for sale by a provider, whether or not the service is encoded or otherwise made unintelligible, without full payment.

~~The requisite intent may be inferred from proof that the person has sold, leased or offered to sell or lease any such device, plan or kit and stated or implied to the buyer or lessee that it will enable the buyer or lessee to obtain an information service without charge.~~

~~(g) Possess any other materials for the purpose of creating a device or a kit for a device designed to obtain an information service in any manner prohibited pursuant to this section.~~

~~2. This section does not prohibit or restrict a holder of an amateur service license issued by the Federal Communications Commission from possessing or using a radio receiver or transceiver that is intended primarily for use in the amateur radio service and is used for lawful purposes.~~

~~3. A person who violates any provision of this section is guilty of a category D felony and shall be punished as provided in NRS 193.130.~~

~~(Added to NRS by 1993, 871; A 1997, 491; 1999, 2710)~~

NRS 205.4765 Individual unlawful tampering with a computer, computer equipment, data therein, or network communications causing damages under $1000, without malice.

1. Any person who knowingly and willfully unlawfully tampers with a computer, its equipment, data therein, or network transmissions, causing damage under $1000 is guilty of a misdemeanor.

NRS 205.4766 Individual unlawful tampering with a computer, computer equipment, data therein, or network communications causing damages under $1000, with malice.

1. Any person who knowingly, willfully, and maliciously unlawfully tampers with a computer, its equipment, data therein, or network transmissions, causing damage under $1000 is guilty of a gross misdemeanor.

NRS 205.4767 Individual unlawful tampering with a computer, computer equipment, data therein, or network communications causing damages over $1000 and with malice, or to enable the commission of other crime.

1. Any person who knowingly, willfully, and maliciously unlawfully tampers with a computer, its equipment, data therein, or network transmissions, as defined causing damage in excess of $1000, or with the intention of thereby committing fraud, extortion, blackmail, vandalism, theft, harassment, or espionage, is guilty of a Class D felony.

NRS 205.4768 Conspiracy to unlawfully tamper with a computer, computer equipment, data therein, or network communications to enable the commission of other crime.

1. Two or more persons who have knowingly, intentionally, and maliciously agreed to unlawfully tamper with a computer, its equipment, data therein, or network transmissions, as defined, with the intention of thereby committing fraud, extortion, blackmail, vandalism, theft, harassment, or espionage, are guilty of a Class C felony exactly when one or more of said persons attempts said tampering.

NRS 205.477 NRS 205.4775 Nevadans' declaration of an expectation of privacy in the digital age.

1. Nevadans hereby declare an expectation of privacy with respect to the following:

(a) The *content* of any digital communication;

(b) Peripheral data such as keystrokes, on-board sensor information, camera and microphone data, screen output, without limitation.

(c) Network identifiers such as hostnames, usernames, IP addresses, MAC addresses, and other device or user identifiers, understood not to include the kinds of divulging of information necessary for networks and computer systems to function normally;

(d) Metadata contextualizing a given digital connection or communication – i.e. timestamps, latency, duration, location data, path-taken, etc.

NRS 205.4771 Requirement of information services engaging in any digital storage of Nevadans' user data to anonymize said data, consistent with industry best-practices.

1. Any information service engaging in any digital storage of Nevadans' user data which does not anonymize the identifiers of such data, as defined, in accordance with industry best-practices, no later than six months after which the data was initially stored, should the service choose to retain it, unless otherwise established by the expressed knowledge and consent of the user, is guilty of a misdemeanor punishable by no less than $250 per offense.

NRS 205.4772 Prohibition of information services engaging in any digital storage of Nevadans' user data to transmit, trade, or sell non-anonymized user data.

1. Any information service engaging in any digital storage of Nevadans' user data which transmits, trades, or sells said data prior to its anonymization, should the service choose to retain it, unless otherwise established by the expressed knowledge and consent of the user, as defined, is guilty of a gross misdemeanor punishable by no less than $750 per offense.

NRS 205.4773 Requirement of information services engaging in any digital storage of Nevadans' medical, financial, legal, and educational records, to encrypt said data, consistent with industry best-practices.

1. Any information service engaging in any digital storage of Nevadans' medical, financial, legal, or educational records which does not encrypt the data in accordance with best-practices

before storing or transmitting it to an authorized party, as defined, is guilty of a gross misdemeanor punishable by no less than $1,000 per offense.

NRS 205.4774 Requirement of information services engaging in any digital storage of Nevadans' communications data to encrypt said data prior to storing it, consistent with industry best-practices, unless otherwise established by the expressed knowledge and consent of the user.

1. Any information service engaging in any digital storage of Nevadans' communications data which does not encrypt said data in accordance with best-practices prior to storing it, unless otherwise established by the expressed knowledge and consent of the user, is guilty of a misdemeanor punishable by no less than $500 per offense.

NRS 205.4776 Requirement of information services to disclose user data upon request of users.

1. Any Information service engaging in any storage of Nevadans' user data, or who in the past engaged in the storage of user data concerning a person who is now or was at the time of storage a citizen or resident of Nevada, must respond to requests by users to disclose, in full physical or digital form, and at no cost to the user, what, if any, non-anonymized user data the service retained about said user at the time of the request.

(a) Legal guardians may request disclosure on behalf of the persons over whom they have guardianship.

(b) Failure to comply with this statute within a reasonable time is a misdemeanor punishable by no less than $500 per offense.

NRS 205.4775 Limit on information services regarding the time said services can retain user data even with the consent of the user.

format seems to be:<6 spaces>NRS<1 space>xxx.xxxx<2 spaces>

then:<6 spaces><number.><4 spaces>

NRS 205.509 Presumption of authority of employee. An employee is presumed to have the authority to access and use:

1. A computer, system or network owned or operated by his or her employer; and

2. Any supporting document to and any data, information, image, program, signal or sound contained in such a computer, system or network,

 unless the presumption is overcome by clear and convincing evidence to the contrary.

(Added to NRS by 1991, 50; A 1999, 2710)—(Substituted in revision for NRS 205.485)

NRS 205.511 Victim authorized to bring civil action.

1. Any victim of a crime described in NRS 205.473 to 205.513, inclusive, may bring a civil action to recover:

(a) Damages for any response costs, loss or injury suffered as a result of the crime;

(b) Punitive damages; and

(c) Costs and reasonable attorney's fees incurred in bringing the civil action.

2. A victim of a crime described in NRS 205.473 to 205.513, inclusive, may bring a civil action pursuant to this section whether or not the person who committed the crime is or has been charged with or convicted or acquitted of the crime or any other offense arising out of the facts surrounding the crime.

3. The provisions of this section do not abrogate or limit the right of a victim of a crime described in NRS 205.473 to 205.513, inclusive, to bring a civil action pursuant to any other statute or the common law.

(Added to NRS by 1999, 2706; A 2001, 1244)

NRS 205.513 Enforcement of provisions.

1. If it appears that a person has engaged in or is about to engage in any act or practice which violates any provision of NRS 205.473 to 205.513, inclusive, the Attorney General or the appropriate district attorney may file an action in any court of competent jurisdiction to prevent the occurrence or continuance of that act or practice.

2. An injunction:

(a) May be issued without proof of actual damage sustained by any person.

(b) Does not preclude the criminal prosecution and punishment of a violator.

(Added to NRS by 1991, 50; A 1999, 2710; 2001, 1244)