S T A T E O F N E W Y O R K

7358

I N S E N A T E

May 14, 2014

Introduced by Sen. GOLDEN -- read twice and ordered printed, and when printed to be committed to the Committee on Energy and Telecommunications

AN ACT to amend the executive law, the general business law and the state technology law, in relation to the New York state online privacy act

THE PEOPLE OF THE STATE OF NEW YORK, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

Section 1. The executive law is amended by adding a new article 10-A to read as follows:

ARTICLE 10-A

OFFICE OF PRIVACY PROTECTION

SECTION 205. OFFICE OF PRIVACY PROTECTION; CREATED.
205-A. ADMINISTRATION.
205-B. PRIVACY PROTECTION ADVISORY COMMITTEE.
205-C. RESPONSIBILITIES.
205-D. CONSTRUCTION.
205-E. REPORT.

S 205. OFFICE OF PRIVACY PROTECTION; CREATED. THE OFFICE OF PRIVACY PROTECTION IS HEREBY CREATED IN THE EXECUTIVE DEPARTMENT. ITS PURPOSE SHALL BE TO PROMOTE AND PROTECT THE PRIVACY OF PERSONAL INFORMATION OF INDIVIDUALS.

S 205-A. ADMINISTRATION. THE OFFICE SHALL BE HEADED BY A COMMISSIONER OF PRIVACY PROTECTION WHO SHALL BE APPOINTED BY THE GOVERNOR BY AND WITH THE ADVICE AND CONSENT OF THE SENATE, AND WHO SHALL HOLD OFFICE AT THE PLEASURE OF THE GOVERNOR. THE COMMISSIONER SHALL POSSES SUCH RIGHTS, POWERS, AND DUTIES IN CONNECTION WITH PRIVACY PROTECTION AS ARE EXPRESSED OR REASONABLY IMPLIED BY THIS CHAPTER OR OTHER APPLICABLE LAWS OF THIS STATE RELATING TO THE ONLINE PRIVACY OF INDIVIDUALS.

S 205-B. PRIVACY PROTECTION ADVISORY COMMITTEE. THERE IS HEREBY CREATED THE PRIVACY PROTECTION ADVISORY COMMITTEE, WHICH SHALL CONSIST OF THE FOLLOWING EX OFFICIO MEMBERS OR THEIR DESIGNEES: THE SECRETARY OF STATE, THE ATTORNEY GENERAL, THE COMMISSIONER OF THE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES, AND THE DIRECTOR OF THE OFFICE OF

EXPLANATION--Matter in ITALICS (underscored) is new; matter in brackets [ ] is old law to be omitted.

LBD14411-04-4

INFORMATION TECHNOLOGY SERVICES. IN ADDITION, THERE SHALL BE APPOINTED BY THE GOVERNOR BY AND WITH THE ADVICE AND CONSENT OF THE SENATE, FIVE PERSONS WHO HAVE BEEN EMPLOYED AT THE LEVEL OF EXECUTIVE OFFICER IN COMPANIES IN THE INFORMATION TECHNOLOGY INDUSTRY FOR A PERIOD OF FIVE YEARS OR MORE OR AS A PRIVACY COMPLIANCE OFFICER FOR SUCH PERIOD, OR AS A CONSULTANT OR ACADEMIC RESEARCHER OR TEACHER OR LAWYER OR HOLDING A SIMILAR POSITION REQUIRING EXPERTISE IN THE FIELD OF PRIVACY AND INFORMATION TECHNOLOGY FOR A PERIOD OF FIVE YEARS OR MORE. THE DIRECTOR OF THE OFFICE OF INFORMATION TECHNOLOGY SERVICES SHALL BE CHAIR OF THE ADVISORY COMMITTEE.

EACH MEMBER OF THE COMMITTEE SHALL BE APPOINTED FOR TERMS OF TWO YEARS. ANY MEMBER MAY BE REAPPOINTED FOR ADDITIONAL TERMS. THE ADVISORY COMMITTEE SHALL MEET NO LESS THAN THREE TIMES EACH YEAR, OR MORE IF ITS BUSINESS REQUIRES. THE ADVISORY COMMITTEE SHALL ADVISE THE COMMISSIONER ON ALL MATTERS RELATING TO PRIVACY CONCERNS, AND ON SUCH OTHER MATTERS AS THE COMMISSIONER SHALL REQUEST. MEMBERS OF THE ADVISORY COMMITTEE SHALL RECEIVE NO COMPENSATION BUT SHALL BE ENTITLED TO ACTUAL AND NECESSARY TRAVELING AND OTHER EXPENSES WHILE ENGAGED IN THE PERFORMANCE OF SUCH MEMBER'S DUTIES HEREUNDER.

THE COMMITTEE SHALL HAVE THE FOLLOWING FUNCTIONS, POWERS AND DUTIES:

1. TO REVIEW AND COMMENT, AS IT DEEMS APPROPRIATE, ON ALL PROPOSED RULES AND REGULATIONS OF THE OFFICE;

2. TO PROVIDE GUIDANCE AND SUPPORT TO THE OFFICE IN THE DEVELOPMENT OF PRIVACY POLICIES OR RECOMMENDATIONS;

3. TO MAKE RECOMMENDATIONS CONCERNING SURVEYS AND REPORTS; AND

4. TO PERFORM SUCH OTHER ACTS AS MAY BE ASSIGNED BY THE CHAIR OF THE COMMITTEE WHICH ARE NECESSARY OR APPROPRIATE TO CARRY OUT THE FUNCTIONS OF THE COMMITTEE.

S 205-C. RESPONSIBILITIES. THE OFFICE OF PRIVACY PROTECTION SHALL:

1. RECEIVE COMPLAINTS CONCERNING VIOLATIONS OF ARTICLES THIRTY-NINE-H AND THIRTY-NINE-F OF THE GENERAL BUSINESS LAW AND VIOLATIONS OF OTHER PRIVACY-RELATED LAWS, INCLUDING IDENTITY THEFT AND IDENTIFY FRAUD, AND SECTIONS THREE HUNDRED NINETY-NINE-DDD AND THREE HUNDRED NINETY-NINE-DDDD OF THIS CHAPTER, AND SHALL REFER, WHERE APPROPRIATE, SUCH COMPLAINTS TO LOCAL, STATE, OR FEDERAL AGENCIES WHERE SUCH AGENCIES ARE AVAILABLE TO ASSIST, AND REQUEST REGULAR UPDATES ON ACTIVITIES UNDERTAKEN DUE TO SUCH REFERRALS FROM SUCH AGENCIES. SUCH AGENCIES TO WHICH COMPLAINTS HAVE BEEN REFERRED SHALL RESPOND TO ANY SUCH REQUESTS FOR UPDATES EXPEDITIOUSLY OR SHALL PROVIDE THE OFFICE WITH A WRITTEN SUMMARY OF REASONS WHY IT COULD NOT COMPLY WITH THE REQUEST;

2. PROVIDE INFORMATION, AND REFERRAL TO INDIVIDUALS AND ENTITIES ABOUT OBTAINING, COMPILING, MAINTAINING, USING, DISCLOSING, OR DISPOSING OF PERSONALLY IDENTIFIABLE INFORMATION IN A LAWFUL MANNER PURSUANT TO ARTICLES THIRTY-NINE-H AND THIRTY-NINE-F OF THIS CHAPTER, INCLUDING THE USE OF AND DISCLOSURE OF SOCIAL SECURITY NUMBERS PURSUANT TO SECTIONS THREE HUNDRED NINETY-NINE-DDD AND THREE HUNDRED NINETY-NINE-DDDD OF THE GENERAL BUSINESS LAW;

3. DEVELOP INFORMATIONAL AND EDUCATIONAL PROGRAMS AND MATERIALS TO FOSTER AND IMPROVE PUBLIC UNDERSTANDING CONCERNING THE ISSUES RELATED TO PRIVACY; AND

4. ASSIST AS REQUESTED IN THE TRAINING OF LOCAL, STATE, AND FEDERAL LAW ENFORCEMENT AGENCIES REGARDING IDENTITY THEFT AND OTHER PRIVACY-RELATED CRIMES.

S 205-D. CONSTRUCTION. THE AUTHORITY OF THE OFFICE OF PRIVACY PROTECTION TO ADOPT REGULATIONS UNDER THIS ARTICLE SHALL BE LIMITED EXCLUSIVELY TO THOSE REGULATIONS NECESSARY TO IMPLEMENT SUBDIVISIONS ONE

THROUGH FOUR OF SECTION TWO HUNDRED FIVE-C OF THIS ARTICLE. NOTHING CONTAINED HEREIN SHALL BE DEEMED TO APPLY TO THE LEGISLATURE OR THE JUDICIARY, OR, EXCEPT AS PROVIDED IN ARTICLES THIRTY-NINE-F AND THIRTY-NINE-H OF THIS CHAPTER, TO A STATE AGENCY AS SUCH TERM IS DEFINED BY SECTION ONE HUNDRED ONE OF THE NEW YORK STATE TECHNOLOGY LAW.

S 205-E. REPORT. THE OFFICE SHALL REPORT ANNUALLY ON THE THIRTIETH OF JANUARY EACH YEAR TO THE GOVERNOR, THE TEMPORARY PRESIDENT OF THE SENATE, THE SPEAKER OF THE ASSEMBLY, THE MINORITY LEADERS OF THE SENATE BEGINNING IN THE FIRST CALENDAR YEAR AFTER THE EFFECTIVE DATE OF THIS SECTION.

1. THE NUMBER OF COMPLAINTS RECEIVED AND THE REFERRALS MADE BY CATEGORY OR CLASS OF COMPLAINT.

2. THE NUMBERS OF INVESTIGATIONS UNDERTAKEN BY THE OFFICE, THE CATEGORIES OF SUCH INVESTIGATIONS, AND THE NUMBERS OF CLOSED CASES OF SUCH INVESTIGATIONS.

3. RECOMMENDATIONS CONCERNING IMPROVEMENTS IN PRIVACY LAWS AND PROCEDURES.

S 2. Section 399-ddd of the general business law, as added by chapter 372 of the laws of 2012, is renumbered section 399-dddd.

S 3. Article 40 and sections 900 and 901 of the general business law, as renumbered by chapter 407 of the laws of 1973, are renumbered article 45 and sections 950 and 951.

S 4. The general business law is amended by adding a new article 39-H to read as follows:

ARTICLE 39-H

NEW YORK STATE ONLINE PRIVACY ACT

SECTION 900. SHORT TITLE.
901. DEFINITIONS.
902. PURPOSE, APPLICATION, EXCEPTIONS, AND WAIVER.
903. REQUIREMENT FOR PRIVACY POLICY AND CONFIDENTIALITY.
904. PRIVACY PROTECTION FOR MINORS.
905. RESPONSIBILITIES CONCERNING PRIVACY POLICIES AND SOCIAL MEDIA.
906. REQUIREMENT TO REPORT A SECURITY BREACH.
907. LIABILITY FOR FAILURE TO COMPLY.
908. ENFORCEMENT.

S 900. SHORT TITLE. THIS ARTICLE SHALL BE KNOWN AND MAY BE CITED AS THE "NEW YORK STATE ONLINE PRIVACY ACT".

S 901. DEFINITIONS. AS USED IN THIS ARTICLE, THE FOLLOWING TERMS SHALL HAVE THE FOLLOWING MEANINGS:

1. "COLLECT" MEANS TO RECEIVE AND STORE INFORMATION, INCLUDING VIA COOKIE TECHNOLOGY, FOR PURPOSES OF RETRIEVAL IN ORDER TO INITIATE COMMUNICATION WITH OR MAKE DETERMINATIONS ABOUT THE PERSON WHO IS THE SUBJECT OF SUCH INFORMATION.

2. "COLLEGE" AND "UNIVERSITY" SHALL HAVE THE SAME MEANINGS AS SET FORTH IN SECTION TWO OF THE EDUCATION LAW.

3. "DISCLOSE" MEANS TO REVEAL, RELEASE, TRANSFER, DISSEMINATE OR OTHERWISE COMMUNICATE INFORMATION ORALLY, IN WRITING, OR BY ELECTRONIC OR OTHER MEANS, TO SOME PERSON OR ENTITY OTHER THAN TO THE PERSON WHO IS THE SUBJECT OF SUCH INFORMATION.

4. "MINOR" MEANS A NATURAL UNEMANCIPATED PERSON SIXTEEN YEARS OF AGE OR LESS WHO RESIDES IN THIS STATE AND IS NOT OTHERWISE INCLUDED IN RULES ISSUED BY THE FEDERAL TRADE COMMISSION PURSUANT TO THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT.

5. "OPERATOR" MEANS A PERSON OR ENTITY THAT OWNS OR OPERATES A WEBSITE OR ONLINE SERVICE THAT COLLECTS PERSONALLY IDENTIFIABLE INFORMATION FROM

A USER RESIDING IN THIS STATE WHO USES OR VISITS SUCH WEBSITE OR ONLINE SERVICE. IT DOES NOT INCLUDE A THIRD PARTY THAT HOSTS BUT DOES NOT OWN A WEBSITE OR ONLINE SERVICE ON BEHALF OF AN OPERATOR OR THAT PROCESSES INFORMATION ON BEHALF OF AN OWNER OR OPERATOR.

6. "PERSONALLY IDENTIFIABLE INFORMATION" INCLUDES THE CATEGORIES OF INFORMATION DESCRIBED IN THIS SUBDIVISION, BUT DOES NOT INCLUDE PUBLICLY AVAILABLE INFORMATION LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS. PERSONALLY IDENTIFIABLE INFORMATION INCLUDES BUT IS NOT LIMITED TO THE FOLLOWING ITEMS OR ANY COMBINATION THEREOF:

(A) FIRST NAME;

(B) LAST NAME;

(C) HOME OR OTHER PHYSICAL ADDRESS;

(D) AGE;

(E) DATE OF BIRTH;

(F) NAMES, AGE, GENDER, TELEPHONE NUMBER OR ELECTRONIC MAIL OR OTHER ADDRESSES OF CHILDREN;

(G) HEIGHT, WEIGHT, RACE, RELIGION, OCCUPATION, OR POLITICAL PARTY AFFILIATION;

(H) E-MAIL ADDRESS;

(I) TELEPHONE NUMBER;

(J) SOCIAL SECURITY NUMBER;

(K) INFORMATION PERTAINING TO BANK ACCOUNTS, INVESTMENT ACCOUNTS, CREDIT OR DEBIT CARDS, OR BALANCES OR ACCOUNT NUMBERS OF ANY OF THESE;

(L) ANY SECURITY CODE, ACCESS CODE, OR PASSWORD THAT WOULD PERMIT ACCESS TO AN INDIVIDUAL'S FINANCIAL ACCOUNT OR OTHER ONLINE ACCOUNT;

(M) MEDICAL INFORMATION, INCLUDING ANY INFORMATION REGARDING AN INDIVIDUAL'S MEDICAL HISTORY, MENTAL OR PHYSICAL CONDITION, OR MEDICAL TREATMENT OR DIAGNOSIS BY A HEALTH CARE PROFESSIONAL, INCLUDING DRUGS, THERAPIES, OR MEDICAL PRODUCTS OR EQUIPMENT USED; AND

(N) HEALTH INSURANCE INFORMATION, INCLUDING AN INDIVIDUAL'S HEALTH INSURANCE POLICY NUMBER OR SUBSCRIBER IDENTIFICATION NUMBER, ANY UNIQUE IDENTIFIER USED BY A HEALTH CARE INSURER TO IDENTIFY THE INDIVIDUAL, OR ANY INFORMATION IN AN INDIVIDUAL'S APPLICATION AND CLAIMS HISTORY, INCLUDING ANY APPEALS RECORDS.

7. "POSTED" MEANS INFORMATION THAT CAN BE ACCESSED BY ANOTHER USER OR USERS IN ADDITION TO THE ORIGINAL USER WHO POSTED THE INFORMATION, IRRESPECTIVE OF WHETHER SUCH ADDITIONAL USER OR USERS ARE REGISTERED USERS OF THE WEBSITE OR ONLINE SERVICE WHERE THE INFORMATION IS POSTED.

8. "PUBLICLY POST" OR "PUBLICLY DISPLAY" MEANS TO INTENTIONALLY COMMUNICATE OR OTHERWISE MAKE AVAILABLE TO THE GENERAL PUBLIC.

9. "CONSPICUOUSLY POST" WITH RESPECT TO A PRIVACY POLICY INCLUDES POSTING ON OR THROUGH ANY OF THE FOLLOWING:

(A) A WEB PAGE ON WHICH THE PRIVACY POLICY IS POSTED IF THE WEB PAGE IS THE HOMEPAGE OR FIRST SIGNIFICANT PAGE A USER ENCOUNTERS ON ENTERING THE WEBSITE;

(B) AN ICON OR TEXT LINK THAT HYPERLINKS TO A WEB PAGE ON WHICH THE PRIVACY POLICY IS POSTED, IF THE ICON IS LOCATED ON THE HOMEPAGE OR THE FIRST SIGNIFICANT PAGE AFTER ENTERING THE WEBSITE, AND IF THE ICON CONTAINS THE WORDS "PRIVACY POLICY." THE ICON SHALL ALSO USE A COLOR THAT CONTRASTS WITH THE BACKGROUND COLOR OF THE WEB PAGE AND IS SET IN TYPE EQUAL TO OR GREATER IN SIZE THAN THE SURROUNDING TEXT ON THE WEBSITE OR IS OTHERWISE DISTINGUISHABLE. IF A TEXT LINK, THEN THE LINK MUST INCLUDE THE WORDS "PRIVACY POLICY" IN CAPITAL LETTERS EQUAL TO OR GREATER IN SIZE AND IN FONT AND COLOR THAT CONTRASTS WITH THE SURROUNDING TEXT; OR

(C) IN THE CASE OF AN ONLINE SERVICE, ANY OTHER REASONABLY ACCESSIBLE MEANS OF MAKING THE PRIVACY POLICY AVAILABLE FOR USERS OF THE ONLINE SERVICE.

10. "PRIVACY POLICY" MEANS A POLICY CONCERNING THE PRIVACY OF PERSONALLY IDENTIFIABLE INFORMATION COLLECTED BY AN OPERATOR THROUGH ITS WEBSITE OR ONLINE SERVICE THAT DOES THE FOLLOWING:

(A) IDENTIFIES THE CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION THAT THE OPERATOR COLLECTS THROUGH THE WEBSITE OR ONLINE SERVICE ABOUT USERS WHO USE OR VISIT ITS WEBSITE OR ONLINE SERVICE AND THE USE OF THAT INFORMATION;

(B) STATES THE MEANS BY WHICH PERSONALLY IDENTIFIABLE INFORMATION IS COLLECTED AND WHETHER SUCH COLLECTION OCCURS ACTIVELY OR PASSIVELY, AND WHETHER SUCH COLLECTION IS VOLUNTARY AND THE CONSEQUENCES, IF ANY, OF A REFUSAL TO PROVIDE THE INFORMATION;

(C) IDENTIFIES THE CATEGORIES OF THIRD-PARTY PERSONS OR ENTITIES WITH WHOM THE OPERATOR MAY SHARE PERSONALLY IDENTIFIABLE INFORMATION;

(D) DISCLOSES WHETHER OTHER PARTIES MAY COLLECT PERSONALLY IDENTIFIABLE INFORMATION ABOUT A USER'S ACTIVITIES OVER TIME AND ACROSS DIFFERENT WEBSITES AND ONLINE SERVICES WHEN SUCH USER CONNECTED TO THE OPERATOR'S WEBSITE OR SERVICE;

(E) STATES WHETHER ANY PERSONALLY IDENTIFIABLE INFORMATION COLLECTED WILL BE RETAINED BY THE OPERATOR, AND, IF SO, THE CATEGORIES OF SUCH PERSONALLY IDENTIFIABLE INFORMATION RETAINED AND THE PERIOD OF TIME OVER WHICH IT WILL BE RETAINED, THE STEPS THE OPERATOR TAKES TO PROTECT THE CONFIDENTIALITY AND INTEGRITY OF THE INFORMATION, INCLUDING THE CATEGORIES OF CONTROLS OF CLOUD SECURITY ARCHITECTURE IF INFORMATION IS STORED ON THE CLOUD, AND THE OPERATOR'S PROCEDURE FOR DESTROYING SUCH INFORMATION ON TERMINATION OF THE USER'S SUBSCRIPTION OR CANCELLATION OF ACCESS TO OR USE OF THE WEBSITE OR THE ONLINE SERVICE;

(F) DESCRIBES THE PROCEDURES BY WHICH A USER MAY GAIN ACCESS TO HIS OR HER PERSONALLY IDENTIFIABLE INFORMATION, AND WHETHER THE OPERATOR MAINTAINS A PROCESS FOR A USER TO REVIEW AND MAKE, OR REQUEST AND OBTAIN, CHANGES TO ANY SUCH PERSONALLY IDENTIFIABLE INFORMATION COLLECTED THROUGH THE WEBSITE OR ONLINE SERVICE. IF THERE IS SUCH A PROCESS, THE OPERATOR SHALL PROVIDE A DESCRIPTION OF THAT PROCESS. IF AN OPERATOR COLLECTS SUCH INFORMATION BUT DOES NOT PROVIDE A MEANS FOR A USER OF ITS WEBSITE OR ONLINE SERVICE TO OBTAIN SUCH CHANGES, IT SHALL CONSPICUOUSLY POST THE STATEMENT, "THIS WEBSITE OR ONLINE SERVICE COLLECTS PERSONALLY IDENTIFIABLE INFORMATION FROM ITS USERS AND DOES NOT ALLOW THE USER TO REVIEW OR CHANGE SUCH INFORMATION";

(G) DESCRIBES THE PROCESS BY WHICH THE OPERATOR NOTIFIES USERS OF MATERIAL CHANGES TO THE OPERATOR'S PRIVACY POLICY FOR THAT WEBSITE OR ONLINE SERVICE; AND

(H) DISCLOSES HOW THE OPERATOR RESPONDS TO WEB BROWSER "DO NOT TRACK" SIGNALS OR OTHER MECHANISMS THAT ALLOW USERS TO EXERCISE CHOICE REGARDING THE COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION. AN OPERATOR MAY SATISFY THIS REQUIREMENT BY PROVIDING A CLEAR AND CONSPICUOUS HYPERLINK IN THE OPERATOR'S PRIVACY POLICY TO AN ONLINE LOCATION CONTAINING A DESCRIPTION, INCLUDING THE EFFECTS, OF ANY PROGRAM OR PROTOCOL THE OPERATOR FOLLOWS THAT OFFERS THE USER TO EXERCISE SUCH CHOICE.

11. "SOCIAL MEDIA" MEANS AN INTERNET-BASED SERVICE THAT ALLOWS INDIVIDUALS TO ENGAGE IN ACTIVITIES WHICH INCLUDE BUT ARE NOT LIMITED TO THE FOLLOWING: CONSTRUCT A PUBLIC OR SEMI-PUBLIC PROFILE WITHIN A BOUNDED SYSTEM, CREATED BY THE SERVICE; CREATE A LIST OF OTHER USERS WITH WHOM THEY SHARE A CONNECTION WITHIN THE SYSTEM; AND VIEW AND NAVIGATE THEIR LIST OF CONNECTIONS AND THOSE MADE BY OTHERS WITHIN THE SYSTEM. SOCIAL

MEDIA INCLUDES FACEBOOK, E-MAIL, AND TWITTER ACCOUNTS, AND OTHER SIMILAR SERVICES, AND WEBSITES AND ONLINE SERVICES WHICH INCLUDE THE ACTIVITIES DESCRIBED IN THIS SUBDIVISION, AND THE DIGITAL MEDIA CONTAINED IN THOSE SITES, INCLUDING PHOTOS, VIDEOS, TEXTS AND E-MAIL MESSAGES.

12. "SECURITY BREACH" OR "BREACH OF SECURITY" OF THE SYSTEM HAS THE SAME MEANING AS "BREACH OF SECURITY OF THE SYSTEM" AS DEFINED IN ARTICLE THIRTY-NINE-F OF THIS CHAPTER.

13. "USER" MEANS AN INDIVIDUAL WHO USES THE INTERNET TO ACCESS A WEBSITE OR ONLINE SERVICE OR SOCIAL MEDIA.

14. "WEBSITE OR ONLINE SERVICE" MEANS AND INCLUDES A WEBSITE, ONLINE SERVICE, ONLINE APPLICATION, MOBILE APPLICATION, ELECTRONIC SERVICE OR ACCOUNT, THAT CONTAINS ELECTRONIC CONTENT, INCLUDING BUT NOT LIMITED TO VIDEOS, STILL PHOTOGRAPHS, BLOGS, VIDEO BLOGS, PODCASTS, INSTANT AND TEXT MESSAGES, E-MAIL, ONLINE SERVICES OR ACCOUNTS, OR WEBSITE PROFILES OR LOCATIONS.

15. "WEBSITE OR ONLINE SERVICE DIRECTED TO MINORS" MEANS A WEBSITE OR ONLINE SERVICE OR PORTION THEREOF CREATED, DEVELOPED, OR USED FOR THE PURPOSE OF REACHING AN AUDIENCE PREDOMINANTLY COMPRISED OF MINORS, AND NOT DESIGNED OR INTENDED FOR A MORE GENERAL AUDIENCE COMPRISED OF ADULTS; PROVIDED, HOWEVER, THAT REFERRING OR LINKING VIA SUCH INFORMATION LOCATION TOOLS AS A DIRECTORY, INDEX, REFERENCE, POINTER, OR HYPERTEXT LINK TO A WEBSITE, ONLINE SERVICE, ONLINE APPLICATION, OR MOBILE APPLICATION DIRECTED TO MINORS SHALL NOT BE DEEMED TO QUALIFY SUCH WEBSITE OR ONLINE SERVICE AS ONE CREATED, DEVELOPED, OR USED FOR THE PURPOSE OF REACHING AN AUDIENCE PREDOMINANTLY COMPRISED OF MINORS.

S 902. PURPOSE, APPLICATION, EXCEPTIONS, AND WAIVER. 1. THE PURPOSE OF THIS ARTICLE IS TO HELP SAFEGUARD THE PRIVACY OF PERSONALLY IDENTIFIABLE INFORMATION OF USERS OF WEBSITES AND ONLINE SERVICES BY: ESTABLISHING REQUIREMENTS FOR THE CONFIDENTIAL TREATMENT OF SUCH INFORMATION BY THE OPERATORS OF WEBSITES AND ONLINE SERVICES; REQUIRING DISCLOSURE TO USERS OF THE PRIVACY POLICY OF SUCH WEBSITES OR ONLINE SERVICES; PROVIDE TO USERS WHO ARE MINORS OVER THE AGE OF THIRTEEN THE SAME PROTECTION AFFORDED BY THE RULES ISSUED BY THE FEDERAL TRADE COMMISSION PURSUANT TO THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT FOR CHILDREN UNDER THE AGE OF THIRTEEN; TO RESTRICT ACCESS TO SOCIAL NETWORKING INFORMATION OF USERS BY CERTAIN EDUCATIONAL INSTITUTIONS AND EMPLOYERS; TO REQUIRE IMMEDIATE REPORTING OF A SECURITY BREACH OF PERSONALLY IDENTIFIABLE INFORMATION; AND TO ESTABLISH PENALTIES FOR VIOLATIONS.

2. THE PROVISIONS OF THIS ARTICLE SHALL NOT APPLY TO ANY WEBSITE OR ONLINE SERVICE THAT DOES NOT COLLECT PERSONALLY IDENTIFIABLE INFORMATION CONCERNING USERS, ANY AGENCY OR POLITICAL SUBDIVISION OF THE STATE OR THE FEDERAL GOVERNMENT, OR A FINANCIAL INSTITUTION THAT HAS ADOPTED SAFEGUARDS THAT COMPLY WITH THE STANDARDS ESTABLISHED PURSUANT TO SECTION 501(B) OF THE GRAMM-LEACH-BLILEY ACT OF 1999, 15 USC 6801. ANY GROUP DESCRIBED IN THIS SUBDIVISION MAY CONSPICUOUSLY POST A STATEMENT ON ITS WEBSITE OR WITH OR THROUGH ITS ONLINE SERVICE THAT STATES THAT IT DOES NOT COLLECT PERSONALLY IDENTIFIABLE INFORMATION OR IS NOT COVERED BY THE PROVISIONS OF THIS ARTICLE WITH A STATEMENT AS TO THE REASONS FOR SUCH EXCLUSION.

3. ANY OTHER PROVISION OF THIS ARTICLE TO THE CONTRARY NOTWITHSTANDING, AN OPERATOR MAY DISCLOSE PERSONALLY IDENTIFIABLE INFORMATION ON A LIMITED BASIS IF THE DISCLOSURE IS MADE:

(A) PURSUANT TO A COURT ORDER, A GRAND JURY SUBPOENA, OR OTHERWISE PURSUANT TO REQUIREMENTS OF LAW;

(B) TO A COURT IN A CIVIL ACTION FOR CONVERSION COMMENCED BY THE OPERATOR OR IN A CIVIL ACTION TO ENFORCE COLLECTION OF UNPAID SUBSCRIPTION

FEES OR PURCHASE AMOUNTS, AND THEN ONLY TO THE EXTENT NECESSARY TO ESTABLISH THE FACT OF THE SUBSCRIPTION DELINQUENCY OR PURCHASE AGREEMENT, AND WITH APPROPRIATE SAFEGUARDS AGAINST UNAUTHORIZED DISCLOSURE;

(C) FOR THE SOLE PURPOSE OF VALIDATING THE IDENTITY OR CREDIT-WORTHINESS OF THE USER OR FOR A FRAUD INVESTIGATION WHEN MADE TO ANOTHER ENTITY OR WHICH HAS THE EXPERTISE AND ABILITY TO PROVIDE SUCH VALIDATION OR TO A BUSINESS SUBSIDIARY OR RELATED ENTITY IF RESTRICTED TO DISCLOSURE SOLELY FOR A LEGITIMATE BUSINESS REASON;

(D) AT THE REQUEST OF THE USER;

(E) WHEN THE INFORMATION IS TO BE USED FOR ANY BUSINESS FUNCTION PERMITTED OR ALLOWED UNDER THE GRAMM LEACH BLILEY ACT, P.L. 106-102 (1999) BY ANY ENTITY REGULATED BY SUCH ACT;

(F) IN CONNECTION WITH A REQUEST FOR CREDIT OR A CREDIT TRANSACTION INITIATED BY THE USER OR IN CONNECTION WITH A LAWFUL REQUEST FOR A CONSUMER REPORT OR INVESTIGATIVE CONSUMER REPORT, AS SUCH TERMS ARE DEFINED IN SECTION THREE HUNDRED EIGHTY-A OF THIS CHAPTER;

(G) FOR PURPOSES OF EMPLOYMENT, INCLUDING IN THE COURSE OF ADMINISTRATION OF A CLAIM, BENEFIT, OR PROCEDURE RELATED TO THE INDIVIDUAL'S EMPLOYMENT BY THE PERSON, INCLUDING THE INDIVIDUAL'S TERMINATION FROM EMPLOYMENT, RETIREMENT, INJURY SUFFERED DURING THE COURSE OF EMPLOYMENT, OR TO CHECK ON AN UNEMPLOYMENT INSURANCE CLAIM OF THE INDIVIDUAL; OR

(H) SOLELY FOR STATISTICAL PURPOSES AND IS IN A FORM THAT CANNOT BE USED TO IDENTIFY ANY PARTICULAR PERSON.

4. THE PROVISIONS OF THIS ARTICLE SHALL BE EXCLUSIVE AND SHALL PREEMPT ANY PROVISIONS OF LOCAL LAW, ORDINANCE OR CODE, AND NO LOCALITY SHALL IMPOSE REQUIREMENTS THAT ARE INCONSISTENT WITH OR MORE RESTRICTIVE THAN THOSE SET FORTH IN THIS ARTICLE. WITH RESPECT TO SOCIAL SECURITY NUMBERS, THE PROVISIONS OF SECTION THREE HUNDRED NINETY-NINE-DDD AND THREE HUNDRED NINETY-NINE-DDDD OF THIS CHAPTER SHALL BE CONTROLLING.

5. ANY WAIVER OF A PROVISION OF THIS ARTICLE IS CONTRARY TO PUBLIC POLICY AND IS VOID AND UNENFORCEABLE.

S 903. REQUIREMENT FOR PRIVACY POLICY AND CONFIDENTIALITY. 1. AN OPERATOR SHALL CONSPICUOUSLY POST ITS PRIVACY POLICY AND THE EFFECTIVE DATE OF THE POLICY ON ITS WEBSITE, OR IN THE CASE OF AN ONLINE SERVICE, MAKE THE POLICY AVAILABLE VIA E-MAIL OR OTHER ACCESSIBLE NOTIFICATION WHEN THE USER SIGNS INTO THE SERVICE. THE NOTICE SHALL INCLUDE A STATEMENT THAT A USER MAY REQUEST, IN WRITING OR BY E-MAIL, TO HAVE HIS OR HER E-MAIL ADDRESS KEPT CONFIDENTIAL AS REQUIRED BY THIS ARTICLE.

2. EXCEPT AS OTHERWISE PROVIDED IN THIS ARTICLE OR AUTHORIZED BY ANY OTHER SECTION OF LAW, AN OPERATOR SHALL KEEP CONFIDENTIAL AND SHALL NOT SHARE THE FOLLOWING ITEMS OF INFORMATION WITH ANY UNAUTHORIZED PARTY OR ENTITY:

(A) ALL PERSONALLY IDENTIFIABLE INFORMATION CONCERNING A USER, OTHER THAN THE E-MAIL ADDRESS OF THE USER, UNLESS THE USER GIVES PERMISSION, IN WRITING OR BY E-MAIL, TO THE OPERATOR TO DISCLOSE SUCH INFORMATION; AND

(B) THE E-MAIL ADDRESS OF THE USER, IF THE USER SO REQUESTS IN WRITING OR BY E-MAIL. UPON RECEIVING SUCH A REQUEST, AN OPERATOR SHALL KEEP CONFIDENTIAL AND SHALL NOT SHARE WITH ANY UNAUTHORIZED PARTY OR ENTITY THE E-MAIL ADDRESS OF THE USER, UNLESS THE USER GIVES PERMISSION IN WRITING OR BY E-MAIL, TO THE OPERATOR TO DISCLOSE SUCH E-MAIL ADDRESS.

3. OTHER PROVISIONS OF THIS ARTICLE TO THE CONTRARY NOTWITHSTANDING, THE PROVISIONS OF SECTIONS THREE HUNDRED NINETY-NINE-DDD AND THREE HUNDRED NINETY-NINE-DDDD OF THIS CHAPTER CONCERNING SOCIAL SECURITY NUMBERS SHALL APPLY TO WEBSITES AND ONLINE SERVICES, AND SHALL MEAN AND INCLUDE PORTIONS OF SOCIAL SECURITY NUMBERS. ANY PROVISION IN SUCH

SECTIONS OF THIS CHAPTER ALLOWING FOR DISCLOSURE OF A SOCIAL SECURITY NUMBER UPON THE CONSENT OF AN INDIVIDUAL SHALL BE DEEMED TO MEAN THE EXPRESS CONSENT OF THE INDIVIDUAL.

4. AN OPERATOR SHALL DESTROY, ERASE, OR DELETE ANY COMPUTER FILES, DOCUMENTS, OR ELECTRONIC RECORDS CONTAINING PERSONALLY IDENTIFIABLE INFORMATION OF A USER WHO CANCELS THE ONLINE SERVICE OR WEBSITE SUBSCRIPTION, AND SHALL NOTIFY THE USER WHO CANCELS THE ONLINE SERVICE OR WEBSITE SUBSCRIPTION AND SHALL NOTIFY THE USER OF SUCH DESTRUCTION WITHIN FIVE DAYS OF SUCH CANCELLATION.

5. THE VOLUNTARY DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION TO A WEBSITE OR ONLINE SERVICE OF AN OPERATOR, WHETHER SOLICITED OR UNSOLICITED, SHALL BE DEEMED TO CONSTITUTE CONSENT TO THE COLLECTION OF SUCH INFORMATION BY THE OPERATOR SOLELY FOR THE PURPOSES FOR WHICH THE USER DISCLOSED IT, AS REASONABLY ASCERTAINABLE FROM THE NATURE AND TERMS OF THE DISCLOSURE, BUT SHALL NOT BE DEEMED TO CONSTITUTE CONSENT TO DISCLOSURE OF SUCH PERSONALLY IDENTIFIABLE INFORMATION TO ANY OTHER PARTY ABSENT EXPRESS CONSENT AS IS REQUIRED BY THIS ARTICLE OR WHICH IS EXPRESSLY OTHERWISE ALLOWED BY THIS ARTICLE.

S 904. PRIVACY PROTECTION FOR MINORS. AN OPERATOR OF A WEBSITE OR ONLINE SERVICE WHICH IS REQUIRED TO COMPLY WITH THE RULES ISSUED BY THE FEDERAL TRADE COMMISSION PURSUANT TO THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT WITH RESPECT TO MINORS UNDER THE AGE OF THIRTEEN SHALL PROVIDE THE SAME LEVEL OF ACTIVITY, PROTECTION, AND COMPLIANCE TO MINORS AS DEFINED HEREIN IRRESPECTIVE OF WHETHER SUCH WEBSITE OR ONLINE SERVICE OPERATES SOLELY WITHIN THE STATE.

S 905. RESPONSIBILITIES CONCERNING PRIVACY POLICIES AND SOCIAL MEDIA.

1. AN EMPLOYER SHALL NOT REQUIRE OR REQUEST AN EMPLOYEE OR APPLICANT FOR EMPLOYMENT TO DISCLOSE A USERNAME OR PASSWORD FOR THE PURPOSE OF ACCESSING SOCIAL MEDIA, OR TO ACCESS SOCIAL MEDIA IN THE PRESENCE OF THE EMPLOYER, OR TO DIVULGE ANY SOCIAL MEDIA. AN EMPLOYER SHALL NOT DISCHARGE OR DISCIPLINE, OR OTHERWISE RETALIATE AGAINST AN EMPLOYEE OR APPLICANT FOR NOT COMPLYING WITH A REQUEST OR DEMAND BY THE EMPLOYER THAT VIOLATES THIS SUBDIVISION. THE FOREGOING TO THE CONTRARY NOTWITHSTANDING, NOTHING IN THIS SUBDIVISION SHALL AFFECT AN EMPLOYER'S EXISTING RIGHTS AND OBLIGATIONS TO REQUEST AN EMPLOYEE TO DIVULGE SOCIAL MEDIA REASONABLY BELIEVED TO BE RELEVANT TO AN INVESTIGATION OF ALLEGATIONS OF EMPLOYEE MISCONDUCT OR VIOLATION OF APPLICABLE LAWS AND REGULATIONS, PROVIDED THAT THE SOCIAL MEDIA IS USED SOLELY FOR PURPOSES OF SUCH INVESTIGATION OR FOR A RELATED PROCEEDING, OR SHALL BE DEEMED TO PRECLUDE AN EMPLOYER FROM REQUIRING OR REQUESTING AN EMPLOYEE TO DISCLOSE A USERNAME, PASSWORD, OR OTHER METHOD FOR THE PURPOSE OF ACCESSING AN EMPLOYER-ISSUED ELECTRONIC DEVICE, OR TO PROHIBIT AN EMPLOYER FROM TERMINATING OR OTHERWISE TAKING AN ADVERSE ACTION AGAINST AN EMPLOYEE OR APPLICANT AS MAY BE OTHERWISE PERMITTED BY LAW.

2. COLLEGES AND UNIVERSITIES, AND THEIR EMPLOYEES AND REPRESENTATIVES, SHALL NOT REQUIRE OR REQUEST A STUDENT, PROSPECTIVE STUDENT, OR STUDENT GROUP TO DISCLOSE A USER NAME OR PASSWORD FOR ACCESSING SOCIAL MEDIA, OR TO ACCESS SOCIAL MEDIA IN THE PRESENCE OF THE INSTITUTION'S EMPLOYEE OR REPRESENTATIVE, OR TO DIVULGE ANY SOCIAL MEDIA INFORMATION. NO COLLEGE OR UNIVERSITY SHALL SUSPEND, EXPEL, DISCIPLINE, OR OTHERWISE PENALIZE A STUDENT, PROSPECTIVE STUDENT, OR STUDENT GROUP IN ANY WAY FOR REFUSING TO COMPLY WITH A REQUEST OR DEMAND THAT VIOLATES THIS SUBDIVISION, PROVIDED HOWEVER THAT NOTHING CONTAINED IN THIS SUBDIVISION SHALL BE DEEMED TO AFFECT THE RIGHTS AND OBLIGATIONS OF A COLLEGE OR UNIVERSITY TO PROTECT AGAINST AND INVESTIGATE ALLEGED STUDENT MISCONDUCT OR VIOLATIONS OF APPLICABLE LAWS AND REGULATIONS, OR TO PROHIBIT SUCH

INSTITUTION FROM TAKING ANY ADVERSE ACTION AGAINST A STUDENT, PROSPECTIVE STUDENT, OR STUDENT GROUP FOR ANY LAWFUL REASON OR TO PROHIBIT A STUDENT FROM VOLUNTARILY CONSENTING TO SUCH DISCLOSURE. A COLLEGE OR UNIVERSITY SHALL CONSPICUOUSLY POST ITS PRIVACY POLICY INCLUDING ITS PRIVACY POLICY REGARDING SOCIAL MEDIA.

S 906. REQUIREMENT TO REPORT A SECURITY BREACH. WITHIN TWENTY-FOUR HOURS FOLLOWING DISCOVERY OR NOTIFICATION OF A SECURITY BREACH, PURSUANT TO ARTICLE THIRTY-NINE-F OF THIS CHAPTER, AN OPERATOR SHALL INFORM THE OFFICE OF PRIVACY PROTECTION AS TO THE BREACH, THE DATE AND EXTENT OF THE BREACH, THE CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION THAT WERE OR ARE REASONABLY BELIEVED TO HAVE BEEN THE SUBJECT OF THE BREACH, THE NUMBER OF CONSUMERS AFFECTED, THE GEOGRAPHIC AREA OF THE BREACH, AND TOLL-FREE TELEPHONE NUMBERS OF COMPANY REPRESENTATIVES ASSIGNED TO PROVIDE INFORMATION CONCERNING THE BREACH. AN OPERATOR SHALL ADDITIONALLY REPORT A SECURITY BREACH TO THE OFFICE OF INFORMATION TECHNOLOGY SERVICES WITHIN TWENTY-FOUR HOURS OF DISCOVERY OF ANY SECURITY BREACH AND SHALL INCLUDE THE ITEMS OF INFORMATION SPECIFIED IN ARTICLE FOUR OF THE STATE TECHNOLOGY LAW.

S 907. LIABILITY FOR FAILURE TO COMPLY. 1. ANY OPERATOR WHICH IS NEGLIGENT IN FAILING TO COMPLY WITH ANY REQUIREMENT IMPOSED UNDER SECTION NINE HUNDRED THREE OF THIS ARTICLE WITH RESPECT TO A USER OF ITS WEBSITE OR ONLINE SERVICE IS LIABLE TO THAT USER IN AN AMOUNT EQUAL TO THE SUM OF ANY ACTUAL DAMAGES SUSTAINED AS A RESULT OF SUCH FAILURE, AND IN THE CASE OF ANY SUCCESSFUL ACTION TO ENFORCE ANY LIABILITY UNDER THIS SECTION, THE COSTS OF THE ACTION TOGETHER WITH REASONABLE ATTORNEY'S FEES AS DETERMINED BY THE COURT; PROVIDED HOWEVER THAT SOLELY WITH RESPECT TO AN ALLEGED FAILURE TO POST A PRIVACY POLICY, OR TO POST TIMELY, OR TO POST ALL THE INFORMATION REQUIRED, OR TO POST ACCURATE INFORMATION, AN OPERATOR MAY ASSERT AS A COMPLETE DEFENSE IN ANY ACTION IN LAW OR EQUITY THAT IT THEREAFTER PROVIDED SUCH INFORMATION TO ALL AFFECTED USERS WITHIN THIRTY DAYS OF THE DATE THAT OPERATOR KNEW OF SUCH FAILURE.

2. ANY PERSON WHO WILLFULLY VIOLATES THE PROVISIONS OF SUBDIVISION TWO OR THREE OF SECTION NINE HUNDRED THREE OR SECTION NINE HUNDRED SIX OF THIS ARTICLE SHALL BE ADDITIONALLY SUBJECT TO A CIVIL PENALTY NOT TO EXCEED ONE THOUSAND DOLLARS FOR EACH SUCH VIOLATION.

3. ANY OPERATOR WHO KNOWINGLY MAKES A FALSE OR MISLEADING STATEMENT IN A PRIVACY POLICY OR WHO FAILS TO PROVIDE PRIVACY PROTECTION FOR MINORS PURSUANT TO SECTION NINE HUNDRED FOUR AS REQUIRED BY THIS ARTICLE SHALL BE ADDITIONALLY SUBJECT TO A FINE OF FIVE HUNDRED DOLLARS FOR EACH SUCH VIOLATION, PROVIDED SUCH CIVIL PENALTY SHALL NOT EXCEED FIVE HUNDRED THOUSAND DOLLARS FOR ANY SINGLE EVENT.

4. ANY EMPLOYER WHO VIOLATES THE PROVISIONS OF SECTION NINE HUNDRED FIVE OF THIS ARTICLE SHALL BE SUBJECT TO THE CIVIL PENALTIES, REMEDIES, AND PROVISIONS IMPOSED PURSUANT TO SECTION SIX HUNDRED SEVENTY-FIVE OF THIS CHAPTER.

5. THE RIGHTS AND REMEDIES AVAILABLE UNDER THIS SECTION ARE CUMULATIVE TO EACH OTHER AND TO ANY OTHER RIGHTS AND REMEDIES AVAILABLE UNDER LAW.

S 908. ENFORCEMENT. THE ATTORNEY GENERAL OR ANY DISTRICT ATTORNEY MAY APPLY FOR AN ORDER TEMPORARILY OR PERMANENTLY RESTRAINING AND ENJOINING ANY PERSON FROM VIOLATING ANY PROVISION OF THIS ARTICLE.

S 5. The state technology law is amended by adding a new article 4 to read as follows:

ARTICLE 4

BREACH NOTIFICATION SERVICE

SECTION 401. BREACH NOTIFICATION SERVICE.

S 401. BREACH NOTIFICATION SERVICE. THE OFFICE SHALL COLLABORATE WITH THE OFFICE OF PRIVACY PROTECTION TO CREATE A SERVICE TO BE HOUSED WITHIN THE OFFICE UNDER WHICH A COMPANY REQUIRED TO REPORT ON A SECURITY BREACH, AS SUCH TERM IS DEFINED IN ARTICLE THIRTY-NINE-E OF THE GENERAL BUSINESS LAW, SHALL BE REQUIRED TO POST THE FOLLOWING INFORMATION CONCERNING THE BREACH:

1. THE NAME OF THE COMPANY AND CONTACT INFORMATION OF THE OPERATOR OF THE WEBSITE OR SERVICE, WITH THE CONTACT INFORMATION TO INCLUDE A TOLL-FREE NUMBER;

2. THE DATE OF THE SECURITY BREACH AND THE NUMBER OF CONSUMERS AFFECTED;

3. THE GEOGRAPHIC AREA OF THE BREACH; AND

4. TOLL-FREE TELEPHONE NUMBERS AND ADDRESSES OF THE MAJOR CREDIT REPORTING AGENCIES.

THE SERVICE SHALL BE DESIGNED TO PROVIDE ONLINE NOTIFICATION CONCERNING SECURITY BREACHES TO CONSUMERS WHO REQUEST SUCH INFORMATION BASED ON GEOGRAPHY, TYPE OF CREDIT OR BANK CARD, BANKING OR FINANCIAL INSTITUTION, OR OTHER CATEGORIES OF INFORMATION AS SHALL BE PROVIDED IN THE SERVICE.

S 6. This act shall take effect on the one hundred twentieth day after it shall have become a law.