

repercussions; and

WHEREAS, for example, in 2017 Equifax discovered evidence of a cyber-security breach that compromised the sensitive and private consumer information of approximately 148 million United States consumers and approximately 5.4 million Illinoisans; and

WHEREAS, the injury of the breach was compounded by an undue delay in reporting it, exploitative "remedies" from which the company stood to profit, and other allegations of corporate malfeasance; and

WHEREAS, in another example, the City of Chicago sued the software application based ride-share company Uber after it was revealed the company waited more than a year to disclose a massive data breach affecting 57 million customers, and paid the hackers \$100,000 to conceal the incident; and

WHEREAS, on March 17, 2018 both the New York Times and The Guardian reported that political data firm Cambridge Analytica used the personal information of up to 87 million users of social media giant Facebook without permission, and under the pretext of collecting it for academic purposes; and

WHEREAS, these are but a few recent, high profile instances of wide-ranging breaches, yet they serve to evidence a lack of consumer rights and recourses in the realm of data collection and protection; and

WHEREAS, this type of consumer disenfranchisement is exacerbated by emerging information regarding the nature and scope of the work of data brokers; and

WHEREAS, this generally unknown industry harbors billions of data points covering almost every person and sells them for purposes as wide ranging as advertising, fraud detection, pricing insurance products, and performing background checks; and

WHEREAS, in 2017, Forbes Magazine predicted that the big data analytics market would soon surpass \$200 billion from \$130 billion in 2016, noting that "there's gold in them there mountains of data;" and

WHEREAS, more alarming than what is known is what generally is not - when and how personal data collected, for what purpose, and to whom it is disclosed; and

WHEREAS, as deliberate key strokes and screen taps unwittingly make us actors in a global economy, some privacy compromises are effectuated by the mere act of being at a certain location; and

WHEREAS, the popularity and utility of Location Based Service applications and "smart" phones and devices for numerous daily functions such as navigating traffic, finding the nearest restaurant or gas station, or even getting tailored retailer discount offers, promises an enduring tension between privacy and convenience; and

WHEREAS, location information is often collected for targeted advertisement purposes and is therefore a prime commodity between those who collect it and those who stand to benefit from it; and

WHEREAS, here, again, a service provider's efforts to notify a user of the collection and use of data is no more

than perfunctory when it is done in "fine print" or it is merely what users furtively try to click through when they are less concerned with privacy and more concerned with getting directions to a restaurant that they have already bypassed; and

WHEREAS, awareness of the nature and risks of data collection and consent to it must be executed in a manner and time in which of-the-moment needs and concerns are not primordial; and

WHEREAS, personal information in the digital realm is modern-day currency that we all own yet give up, constantly, unwillingly, and unwittingly; and

WHEREAS, it is time to equip consumers with control over their information, informed consent to its disclosure, awareness of its use, and redress for its misuse; and

WHEREAS, acknowledging that we share responsibility for ensuring that business interests thrive, so must we recall that so fundamental a value is privacy that its protection from government intrusion is ensconced in the Bill of Rights - we must take care now not to forsake it without consent and for private gain; now, therefore,

BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF CHICAGO:

SECTION 1. The above recitals are expressly incorporated in and made a part of this ordinance as though fully set forth herein.

SECTION 2. Title 4 of the Municipal Code of Chicago is hereby amended by adding Chapter 4-402 as follows:

Chapter 4-402 Data Collection and Protection Ordinance

ARTICLE I. GENERAL PROVISIONS

4-402-005 Title

This ordinance shall be known as the Chicago Personal Data Collection and Protection Ordinance.

4-402-010 Exclusion

The obligations of this Chapter shall not apply to the United States government, the State of Illinois, or any political subdivision thereof, government corporation, municipal corporation, city, county, municipality, district or other department, bureau, agency, or instrumentality of federal, state, or local government.

4-402-015 Severability ,

If any provision, clause, sentence, paragraph, section or part of this Chapter or application thereof to any person or circumstance, shall for any reason be adjudged by a court of competent jurisdiction to be unconstitutional or invalid, said judgment shall not affect, impair or invalidate the remainder of this Chapter and the application of such provision to other persons or circumstances, but shall be confined in its operation to the provision, clause, sentence, paragraph, section, or part thereof .already involved in the controversy in which such judgment has

been rendered and to the person and circumstances affected thereby.

ARTICLE II. DATA COLLECTION AND DISCLOSURE

4-402-050 Purpose and Intent

The purpose of this Article is to provide for the regulation of operators that collect sensitive customer personal information through the Internet about individual consumers in the City of Chicago.

4-402-055 Definitions

As used in this Article:

- a) "Aggregate customer information" means collective data that relates to a group or category of customers, from which individual customer identities and characteristics have been removed, that is not linked or reasonably linkable to any individual person, household, or device. "Aggregate customer information" does not mean one or more individual customer records that have been de-identified.
- b) "Customer" means an individual residing in Chicago who provides, either knowingly or unknowingly, personal information to a private entity, with or without an exchange of consideration, in the course of purchasing, viewing, accessing, renting, leasing, or otherwise using real or personal property or any interest therein, or obtaining a product or service from the private entity, including advertising or other content.
- c) "Customer personal information" means information collected from or about an individual customer or user of an operator's website or online service that is made available to the operator by a customer or user of the customer's subscription or account solely by virtue of the operator-user relationship, including:
- 1) Name and billing information.
 - 2) Government-issued identifiers, including social security number.
 - 3) Information that would permit the physical or online contacting of an individual, such as physical address, email address, phone number, or Internet Protocol (IP) address.
 - 4) Demographic information such as date of birth, age, gender, race, ethnicity, nationality, religion, or sexual orientation.
 - 5) Financial information.
 - 6) Health information.
 - 7) Information pertaining to minors.
 - 8) Geolocation information.
 - 9) Information from the use of the service, such as Web browsing history, application usage history, content of communications, and origin and destination IP addresses of all traffic.
 - 10) Device identifiers, such as media access control (MAC) address or Internet mobile equipment identity (IMEI).
 - 11) Information concerning a customer or user of the customer's subscription or account that is collected or made available and is maintained in personally identifiable form.
- d) "Operator" means any person or entity that owns a website located on the internet, or an online service, that collects and maintains customer personal information from a customer residing in Chicago who uses or visits the website or online service, if the website or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a website or online service on the owner's behalf or by processing information on behalf of the owner.

4-402-060 Prohibited activities

- a) An operator shall not use, disclose, sell, or permit access to customer personal information, except as provided in this Section.
- b) An operator may use, disclose, sell, or permit access to customer personal information if the customer gives the operator prior opt-in consent, which may be revoked by the customer at any time. The mechanism for requesting and revoking consent under this subsection shall be clear and conspicuous, not misleading, in the language primarily used to conduct business with the customer, and made available to the customer at no additional cost. The mechanism shall also be perpetually available on or through the operator's Internet Website or mobile application if it provides one for account management purposes. If the operator does not have an Internet Website, it shall provide a perpetually available mechanism by another means, such as a toll-free telephone number. The customer's grant, denial, or withdrawal of consent shall be given effect promptly and remain in effect until the customer revokes or limits the grant, denial, or withdrawal of consent.
- c) The request for consent shall disclose to the customer all of the following:
- 1) The types of customer personal information for which the operator is seeking customer approval to use, disclose, sell, or permit access.
 - 2) The purposes for which the customer personal information will be used.
 - 3) The categories of entities to which the operator intends to disclose, sell, or permit access to the customer personal information.
- d) An operator shall not:
- 1) Refuse to serve a customer, or in any way limit services to a customer, who does not provide consent under subsection (b), or
 - 2) Charge a customer a penalty, or penalize a customer in any way, or offer a customer a discount or another benefit based on the customer's decision to provide or not provide consent under subsection (b).
- e) An operator shall disclose the customer personal information of the customer upon written request by the customer to any person designated by the customer.

4-402-065 Exceptions

(a) An operator may use, disclose, or permit access to customer personal information without customer consent, but only to the extent necessary to achieve the stated purpose, in the following circumstances, unless otherwise prohibited by law:

- 1) To provide the operator service from which the information is derived, or services necessary to the provision of that service.
- 2) To comply with legal process or other laws, court orders, or administrative orders.

To initiate, render, bill for, and collect for the operator's service.

- 4) To protect the rights or property of the operator, or to protect customers of those services and other operators from fraudulent, abusive, or unlawful use of, or subscription to, those services.
- 5) To provide location information concerning the customer as follows:
 - i) to a public safety answering point, emergency medical service provider, or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the customer's request for emergency services; or
 - ii) to inform the customer's legal guardian, members of the customer's family, or a person reasonably believed by the operator, to be a close personal friend of the customer, of the customer's location in an emergency situation that involves the risk of death or life-threatening harm; or
 - iii) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

b) Nothing in this Article shall restrict an operator from otherwise lawfully generating an aggregate customer information dataset using customer personal information, or using, disclosing, selling, or permitting access to the aggregate customer information dataset it generated.

c) Unless otherwise prohibited by law, an operator may use, disclose, or permit access to customer personal information to advertise or market the operator's communications-related services to the customer, provided that the customer may opt out of that use, disclosure, or access at any time, and the customer is notified of the right to opt out in a manner that is clear and conspicuous, not misleading, in the language primarily used to conduct business with the consumer, persistently available, and made available to the customer at no additional cost.

4-402-070 Applicability

The requirements of this Article shall apply to operators operating within the City of Chicago when providing service to customers physically located in the City of Chicago.

4-402-075 Right of Action

An aggrieved customer may bring a private cause of action in a court of competent jurisdiction seeking for a violation of this Article and the prevailing plaintiff shall be entitled to recover his or her damages, reasonable attorneys' fees and costs; and other relief, including an injunction, as the Court may deem appropriate. An agreement between the operator and the customer to waive the provisions of this Article is no defense to such action. The remedies in this Section shall be cumulative and in addition to any others available at law or in equity. Provided, however, that

only the department of business affairs and consumer protection may enforce the provisions of Section 4-402-085.

4-402-080 Waivers

Any waiver by the customer of the provisions of this Article shall be deemed contrary to public policy and shall be void and unenforceable.

4-402-085 Violations

Violations of this Article shall be punishable by a fine of not less than \$250.00 nor more than \$1500.00.

4-402-090 Enforcement

This Article shall be enforced by the commissioner of business affairs and consumer protection who will promulgate certain rules and regulations for the enforcement thereof.

ARTICLE III. DATA BREACHES

4-402-100 Definitions As used in this

Article:

"Data collector" is any person or entity including but not limited to, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity or person that, for any purpose, handles, collects, disseminates, or otherwise transacts with nonpublic personal information for its profit, or offers the information to a third party for profit.

"Breach of the security of the system data" or "breach" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to unauthorized disclosure.

"Personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through breach of security:

- A) Social Security number.
- B) Driver's license number or State identification card number.

- C) Account number or credit or debit card number or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- D) Medical information.
- E) Health insurance information.
- F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

2) User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

3) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

4-402-105 Notice of Breach

a) Any data collector who conducts business in Chicago that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to Chicago residents whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay. A delay of fifteen (15) days or more from the discovery shall create a presumption of an unreasonable delay, which may be rebuttable by factors including the investigative requirements of law enforcement and essential requirements of measures needed to determine the scope of the breach and to restore the reasonable integrity of the system.

b) Any data collector who maintains computerized data that includes personal information not owned by the data collector shall notify the owner or licensee of the information of any breach of the security system in the most expedient time possible and without unreasonable delay but shall do so no later than fifteen (15) days following discovery if the personal information was, or is reasonably believed to have been, acquired by a person without valid authorization.

c) In the event that any Chicago residents are to be notified, the data collector shall notify the Commissioner of the Department of Business Affairs and Consumer Protection as to the timing, content, and distribution of the notices and known and potential number of affected persons. Such notice shall be made without delaying notice to affected Chicago residents. The data collector shall use the contact method on file in an attempt to give notice to the affected person or business. The data collector shall make a good faith attempt to contact the individual directly to alert them of the breach.

d) The data collector shall give public notice of the data breach in one or more newspapers of general circulation. Such public notice shall include information related to the breach and where questions may be directed.

e) Both the public and private notice shall specify the method through which affected consumers can obtain information about the breach and specify corrective action.

f) The data collector shall continue to update affected persons as information about the breach is received, as any corrective actions are taken, and as remedies become available, until the consumer opts out of those updates or agrees that the matter has been resolved.

4-402-110 Remedies

a) As part of any remedy or ratification process, a company shall not require purchase or enrollment for a fee to any product or service they offer as part of their normal products for sale.

b) As part of any remedy or ratification process, a data collector shall not require waiver of any legal recourses including, but not limited to, a right to trial or binding arbitration agreement.

c) Nothing in this Article shall be construed to limit the rights and remedies that can or shall be made available to the affected consumer.

4-402-115 Violations

The violation of any of the foregoing Sections of this Article shall be deemed a violation of Section 2-25-090 of this Code and subject to the penalties and fines provided therein. Each day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply. Any data collector who is also a licensee that violates this Article shall be subject to license and revocation proceeding as set forth in Section 4-4-280.

ARTICLE IV. DATA BROKERS

4-402-200 Definitions As used in this

Article:

"Consumer" means an individual with a residential address in the City of Chicago and whose Personal Information is in the possession of a Data Broker.

"Data Broker" means a commercial entity that collects, assembles, and possesses Personal Information concerning Consumers who are not customers or employees of that entity in order to sell, trade, or otherwise share the information.

"Department" means the Department of Business Affairs and Consumer Protection.

"Personal Information" means any information that (i) is in the possession of a Data Broker, (ii)

can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information, and (iii) is linked or linkable by such Data Broker to a specific individual with a residential address in the City of Chicago.

4-402-205 Registration Required

Any Data Broker that maintains Personal Information concerning a Consumer shall register with the City of Chicago's Department of Business Affairs and Consumer Protection.

4-402-210 Information Required of Registrants

No later than February 1 of each year, every Data Broker required to register shall file with the Department a certified written statement on a form prescribed by the Department containing the following information:

- a. The registrant's name and permanent address;
- b. The number of Consumers whose Personal Information the registrant collected in the previous year;
- c. The name and nature of the businesses to which Consumer Personal Information was sold, traded, or otherwise shared in the previous year; and
- d. The registration form shall include a written statement certifying that all information contained therein is true and correct.

4-402-215 Failure to Register

When the Department determines that a Data Broker has failed to register as required in this Article, the Department shall notify the Data Broker, in a manner prescribed by the Department, of the failure to register. If the Data Broker fails to register within sixty (60) days of the notice, the Data Broker shall be fined \$250 for each day after February 1 of the registration year for which the Data Broker has not registered. The Department shall suspend the registration of, and not accept a registration statement from, any Data Broker who owes a fine pursuant to this Section until the fine has been paid in full.

4-402-220 Public Notice

The Department shall make public, in a manner that it deems appropriate, the names of the Registrants, the information they provided, and the names of those who violate the registration requirements of this Section.

ARTICLE V. MOBILE PHONE PRIVACY AWARENESS

4-402-250 Definitions. For purposes of this

Article:

"Cellular phone or mobile device retailer" means any person or entity that sells or leases, or offers to sell or lease, phones to the public where such person or entity is a licensee under Title 4 of this Code.

"Location services functionality" means the ability to identify, track, utilize, or store geographical location information.

"Wireless communication device" means any device through which personal wireless services, as defined in 47 U.S.C. 332(c)(7)(C)(i), are transmitted.

4-402-255 Location Services Notice Requirement.

- (a) A cellular phone or mobile device retailer shall provide to each customer who buys or leases a cell phone or wireless communication device with location services functionality a notice with the following language:

CITY OF CHICAGO LOCATION SERVICES NOTICE AND AWARENESS POSTING

- The City of Chicago requires that you be provided the following notice:
 - The device that you have purchased is equipped with "location services" capabilities.
 - This is a function that you can choose to enable or disable on your phone.
 - Many common device functions and applications ("apps") require that you enable this function.
 - Location services data may be retained by your wireless carrier or internet service provider or the application ("app") services that you use.
 - That data could intentionally or unintentionally become available to third parties without your consent, with examples including disclosure through a legal subpoena processes or illicit "hacking" activity.
 - Refer to the instructions in your phone, user manual, or wireless carrier service provider's agreement or privacy notices for more detailed information about how location services uses your location information and how you can control this function.
- b) The notice required by this Section shall be provided to each customer who buys or leases a cell phone or wireless communication device and shall be prominently displayed at any point of sale where such phones and devices are purchased or leased. The notice provided to each customer shall be on paper, in at least fourteen (14) point font, in a list format exactly as written in paragraph (c), above, and in lettering that contrasts with the background color of the notice. The notice posted at each point of sale shall be in a location and manner clearly visible to the public, in at least twenty (20) point font, on a sign not less than eight and one half (8.5) inches in width and eleven (11) inches in height, and in a color that contrasts with the background color of the sign.
- c) Each phone or device covered under this Section that is sold or leased while in violation of the notice requirements in this Section shall constitute a separate violation of this Section.

Each violation of this Section shall cause the licensee to be fined not less than \$150 but not more than

\$250 per violation.

ARTICLE VI. GEOLOCATION INFORMATION

4-402-300 Definitions For purposes of this Article:

"Geolocation information" means information that: (i) is not the contents of a communication; (ii) is generated by or derived from, in whole or in part, the operation of a mobile device, including, but not limited to, a smart phone, tablet, or laptop computer; and (iii) is sufficient to determine or infer the precise location of that device. "Geolocation information" does not include Internet protocol addresses.

"Location-enabled application" means a software application that is downloaded or installed onto a mobile device and that collects, uses, or stores geolocation information.

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. "Private entity" does not include any governmental agency.

4-402-305 Collection, use, storage, and disclosure of geolocation information

a) A private entity may not collect, use, store, or disclose geolocation information from a location-enabled application on a person's device unless the private entity first receives the person's affirmative express consent after providing clear, prominent, and accurate notice that:

- 1) informs the person that his or her geolocation information will be collected, used, or disclosed; and
- 2) informs the person in writing of the specific purposes for which his or her geolocation information will be collected, used, or disclosed; and
- 3) provides the person a hyperlink or comparably easily accessible means to access the information specified in this subsection.

b) A private entity may collect, use, or disclose geolocation information from a location-enabled application on a person's device without receiving affirmative express consent if the collection or disclosure is:

- (1) to allow a parent or legal guardian to locate his or her minor child provided that said access does not violate the terms of any parental, custody, or guardianship rights or agreements; or
- (2) to allow a court-appointed guardian to locate a legally incapacitated person; or
- (3) for the provision of fire, medical, public safety, or other emergency services; or
- 4) for the limited purpose of providing storage, security, or authentication services; or
- 5) to comply with legal process or other laws, court orders, or administrative orders.

- c) A private entity need not obtain a person's affirmative express consent after the person's initial consent as described in subsection (a) has been obtained, unless the terms previously agreed to under subsection (a)(1)-(2) are materially changed.
- d) Any waiver of the notification and consent provisions of this Section is void, unenforceable, and not a defense of a violation of this Chapter. Any contract relating to the use of a location-enabled application that does not comply with this Section shall be void and unenforceable.
- e) This Article applies to location-enabled applications created or modified after the effective date of this Ordinance.

4-402-310 Right of Action

An aggrieved customer may bring a private cause of action in a court of competent jurisdiction seeking for a violation of this Article and the prevailing plaintiff shall be entitled to recover his or her damages, including the value and profits derived from the unauthorized use of geolocation information, reasonable attorneys' fees and costs; and other relief, including an injunction, as the Court may deem appropriate. The remedies in this Section shall be cumulative and in addition to any others available at law or in equity. Provided, however, that only the department of business affairs and consumer protection may enforce the provisions of Section 4-402-305.

4-402-315 Violations

The violation of any of the foregoing sections shall be punishable by a fine of not less than \$50.00 nor more than \$200.00, and the purchase or download of each application while in violation of this Article shall be deemed a separate offense.

ARTICLE VII. ENFORCEMENT

4-402-320 Rules and Duty to Enforce

This Chapter shall be enforced by the Commissioner of the Department of Business Affairs and consumer protection who will promulgate certain rules and regulations for the enforcement thereof. The Commissioner shall work with the Superintendent of the Chicago Police Department to ensure appropriate methods of recording, reporting, and investigating claimed violations of the provisions of this Chapter.

The Corporation Counsel shall, when notified of a data breach event in potential violation of Article 3, report to the Chairman of the Committee on Finance regarding his or her intent to pursue a remedy in a court of competent jurisdiction.

4-402-325 Violations

Any person violating any of the provisions of this Chapter for which no other penalty is provided shall be fined not less than \$100.00 nor more than \$250.00 for each offense. Each violation shall be considered a separate and distinct offense and shall be regarded as being committed on each day on which such person shall continue or permit any such violation. In addition to any fine provided herein, violation of this Chapter

may be grounds for revocation of any license or permit issued by the City of Chicago to any such violator.

Except where otherwise specified, the remedies of this Chapter shall be cumulative and in addition to any others available at law or in equity.

SECTION 3. Effective Date.

This ordinance shall be in full force and effect one hundred and eight (180) days after its passage and approval.