File #: O2017-3920, **Version:** 1

ORDINANCE x <\<L * '^^N 1

WHEREAS, the City of Chicago ("City") is a home rule municipality as described in Section 6(a) of Article VII of the 1970 Constitution ofthe State of Illinois; and

WHEREAS, pursuant to its home rule power, the City of Chicago may exercise any power and perform any function relating to its government and affairs including the power to regulate for the protection of the public health, safety, morals, and welfare; and

WHEREAS, as technology permeates our lives, so do concerns over the privacy protections afforded to Chicagoans; and

WHEREAS, as a Federal Trade Commission-published article acknowledged, designers of the operating systems upon which we increasingly base our routines, "are balancing trade-offs between functionality, convenience, privacy, and security;" and

WHEREAS, the Federal Trade Commission (FTC), in a 2016 Privacy and Data Security Update, reports that it has initiated over forty general privacy lawsuits including one against a foreign-based mobile advertising company charged with deceptively tracking the locations of "hundreds of millions of consumers - including children - without their knowledge or consent" in geo-targeted advertising; and

WHEREAS, unlike instances in which users knowingly avail themselves of location-dependent services such as global positioning devices (GPS), or willingly offer up their location information, such as when "checking in" at a restaurant through a mobile device application ("app"), other location data collecting instances are far less obvious; 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, for instance, in 2016, the ubiquitous ride-sharing Uber application began requiring access to user location information even when the app was not in use, exemplifying the degree to which a developer or service provider can demand personal data without obvious use or benefit to the end user if their offering is deemed indispensable enough; and

WHEREAS, location data 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, both the devices and carriers that service the devices typically offer standard privacy statements; and

WHEREAS, for example, when enabling the location tracking function on an Android device, it will ask for "location consent," advising that "your phone can share its approximate location with apps and services" and advising the user to "read the privacy policy of any app or service provider you are considering to understand how they collect, use and share your location information before you use them;" and

WHEREAS, in another example, popular cell phone service provider T-Mobile offers a "Location Services" statement on its website that advises, in part of "certain risks" including the "potential for misuse..." and acknowledges that "|n]o mobile device user should be 'tracked' without their knowledge and consent;" and

WHEREAS, these advisory efforts and others like it are laudable, they are not always effective, either because they are "fine printed" on websites or because they are what users furtively click "I agree," "I agree," "I agree" to when they are less concerned with privacy and more concerned with getting directions to the restaurant they have already bypassed; and

WHEREAS, in a report prepared for a 2015 Symposium on Usable Privacy and Security, experts acknowledge that both the timing and location of these privacy notices is important, indicating in part that a notice at "an inopportune time may result in users ignoring that notice," and quoting a White House report stating that "only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent;" and

WHEREAS, the writers note that most privacy policies read like contracts "because regulators aim to enforce them like contracts" and that they may be "purposefully vague to avoid limiting potential future uses of collected data," and they go on to identify "public notices" in addition to a device's "primary notices," as part of an effective and comprehensive system of improving privacy notice and issue awareness; and

WHEREAS, consumer behavior might be altered if they are made aware of the privacy compromises offered to them in a context other than when their immediate and primary goal is to access a particular phone application or feature; and

WHEREAS, although there are "smart" devices with location service capabilities other than phones, phones are what individuals are more likely to have on their person most of the time; and

WHEREAS, as Harvard Business School professor Shoshanna Zuboff notes in the January-February 2017 issue of Harvard Magazine, privacy values in the context of what she labels "Surveillance Capitalism" will give rise to battles to be "fought in legislatures and in the courts;" and

WHEREAS, comparing the issue to the lack of labor protections in the late nineteenth century's Gilded Age, she proposes that "[t]he social challenge now.. .is to insist on a new social contract with its own twenty-first century legislative and regulatory innovations, that harnesses information capitalism to democratic values and norms," and contends that this begins "with deepening social understanding and awareness;" and

WHEREAS, acknowledging that we share responsibility for ensuring that business interests thrive but not at the expense of individual privacy rights; and

WHEREAS, location tracking services and data use is substantial modern-day currency that we all own yet give up, very often, unwillingly and unwittingly; and

WHEREAS, the widely held adage that those with nothing to hide have nothing to fear may well be reminded of another precept apt in these times - that we do not always control how "wrongdoing" is defined and protected behavior now might become prosecutable behavior later; now, therefore,

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

SECTION 1. Chapter 4-4 of the Municipal Code of Chicago is hereby amended by adding Section 4-4-340 as follows:

4-4-340 Location Services Notice Requirement

a) This Section shall be known as the "Mobile Phone Privacy Awareness Act"

b) Definitions. As used in this Section:

a. "Cellular phone or mobile device retailer" 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.

b. "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.

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

(c) 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 or internet service provider or the "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.

c) 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.

d) 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 person found to have violated this Section shall be fined not less than $150 but not more than $250 per violation.