LISA M. BROWNLEE, ESQ.
Mexico

NINTH PRELIMINARY DRAFT –FOR ANY/ALL DISTRIBUTION/PUBLIC POSTING

National Human Rights Commission – Mexico (CNDH)

Copies – Federales, Telmex, others

24 April 2012

Re: Mexico law revisions – Warrantless Real-time Cell phone Geolocation Data Surveillance – Parliamentary Gazette Volume X, Number 3455-II, Tuesday, February 21, 2012 (hereinafter "LeyGeolocalización MX")

This memo sets forth my opinion on LeyGeolocalización MX, as experienced privacy, technology/digital rights legal scholar and practitioner, expatriate resident Mexico. My credentials are provided here. I will be publishing my conclusions in an article to be published next week by Bureau of National Affairs (BNA) *E-Commerce Law Report*, which will receive international distribution and, we anticipate, press coverage. A press conference to present my findings will be held in coordination with the weekly press conferences held by Dr. Eduardo Daniel Jiménez González, Abogado Ambassador, International Lawyer, affiliations Harvard, UNAM, Georgetown, Johns Hopkins.

Top-ranking officials[1] in Mexico's data protection authority, IFAI (Instituto Federal de Acceso a la Información y Protección de Datos) generously met with me on 12 April 2012, and permitted me to present an earlier version of this memo. They kindly reviewed it as promised and timely provided a written response. The written response in its entirety is attached in full. Telmex has also received a copy—hand-delivered by me on 12 April 2012 and indicated possible intention of responding; followup by me forthcoming.

Executive summary

What is LeyGeolocalización MX?

For the purposes of this letter, the key points of LeyGeolocalización MX are as follows:

- Right of Mexican government/law enforcement to collect, *without warrant and in real-time*, user geographical location data from cell phones;
- "Destruction" of existing cellphone user database.

[1] Alejandro del Conde, Data Protection Secretariat, Edgardo Martinez, Directorate General of Standards and Studies, Lina Ornelas, General Director of Self-Regulation, and Arturo Rios, Director of International Affairs, all IFAI who have also received direct copies of this memo.

Why LeyGeolocalización MX?

The goal behind LeyGeolocalización MX is to help mitigate MX crime problems. In particular, LeyGeolocalización MX is intended to enable the Mexican government "to investigate possible crimes (organized crime, kidnapping, extortion, or threats) more effectively."[2] No one can refute the need for and merits of such efforts. Mexico's crime/cartel war is an international shame.[3]

Why LeyGeolocalización MX is wrong.

LeyGeolocalización MX will not cease the bloodshed. It will make it worse. In *theory*, the measures passed would be effective to combat cartels/organized crime. However, in *practice*, these measures suffer from technological defects which will result in an extreme worsening of crime in Mexico. The Mexican public will be put at much greater risk of harm as a result of these reforms, for the reasons herein outlined.

These reforms will not achieve their main intended purposes, to: "to investigate possible crimes (organized crime, kidnapping, extortion, or threats) more effectively and to "inhibit the theft of mobile phones and their use for criminal purposes".[4] Rather, these reforms will put the Mexican public at much greater risk, giving organized crime advantages and access, and irreparably harm this country and its people.

In addition, the measures suffer from Constitutional defects that, aside from the obvious violation of human rights of Mexican citizens, will undoubtedly result in the law's annulment by the Supreme Court, costing millions of pesos to litigate. The goals behind these reforms are honorable. However, LeyGeolocalización MX is bad law and will result in substantial harm..

The defects in the reforms are outlined in more detail below.

1. **LeyGeolocalización MX will harm the public. The technological reform of requiring real-time geolocation data collection/reporting is readily circumvented and will be routinely circumvented by organized crime, putting citizens at even greater risk**
2. **The infiltration of law enforcement by the cartels/organized crime will place the public at severe risk of harm from abuses of warrantless access granted to virtually all public servants from the President down to as-yet undefined "delegees"**
3. **The prior law's requirement of registering all user data as a prerequisite to purchase a cell phone and that database's ready-availability on the black market, coupled with the new law's warrantless real-time warrantless geolocation tracking, equips criminals with unprecedented weapons of massive potential destruction, and places targets at unprecedented vulnerability to harm**

---

[2] Mexico Parliamentary Gazette, year XV, Issue 3455-II, Tuesday, February 21, 2012, http://gaceta.diputados.gob.mx/Gaceta/61/2012/feb/20120221-II.html (last accessed 30 March 2012).
[3] Mexico violence high on NAFTA summit agenda, New Zealand Herald, http://t.co/tf2jOCHD, 1 April 2012.
[4] *Op cit.* fn. 1.

4. **LeyGeolocalización MX is over-reaching and redundant for one of its primary intended purposes, to "inhibit the theft of mobile phones and their use for criminal purposes"**
5. **The legislation violates the Constitutional rights of Mexican citizens**

1. LeyGeolocalización MX will harm the public. The technological reform of requiring real-time geolocation data collection/reporting, is readily circumvented and will be routinely circumvented by organized crime, putting the public at even greater risk

The overwhelming evidence of scientific/engineering research demonstrates that circumvention—primarily in the form of jamming--of geolocation data surveillance is successful. Circumvention measures are not yet able to be defended against.[5] I have reviewed extensive tehnical expert literature as well as conducted interviews. At best, defense against circumvention is far in the future.[6] As stated by one security expert, "there is no securing these phones. Everything you connect with is an avenue of attack." [7]

Another expert opinion is equally persuasive on the ease of circumvention and risk of real-time geolocation tracking:

> *Cellular signals (and the geolocation data that is transmitted by them) are vulnerable to jamming, which would render the tracking of a subject's signal difficult or impossible. An individual who suspects his cell phone is being tracked does not need to be a technical wizard to reduce or even eliminate his signal trail from would-be trackers.*[8]

---

[5] See, Know Your Enemy, Signal Characteristics of Civil GPS Jammer, http://radionavlab.ae.utexas.edu/images/stories/files/papers/jammerCharacterizationGPSWorld_Mitch.pdf; Organised crime 'routinely jamming GPS', http://www.telegraph.co.uk/technology/news/9096080/Organised-crime-routinely-jamming-GPS.html. In reviewing the technical reports and correspondence with which I have been provided, and in view of study of extensive evidence and arguments to the contrary, s*ee e.g. e-mail* Todd Humphreys todd.humphreys@mail.utexas.edu.to author ("[accurate to] nearest tower" data.' So I don't think it's fair to say that our study on GPS jamming is "irrefutable tech evidence of the problems with #LeyGeolocalización MX") . I studied all references from Dr. Humphreys. I remain unconvinced that current GSM tracking is safe from jamming—whether multilateralization/cell tower-based or otherwise. See, Royal Academy of Engineering, "Global Navigation Systems: reliance and vulnerabilities," http://www.raeng.org.uk/news/publications/list/reports/RAoE_Global_Navigation_Systems_Report.pdf; see also, "Straight Talk on Anti-Spoofing: Securing the Future of PN http://radionavlab.ae.utexas.edu/images/stories/files/papers/antiSpoofStraightTalk_Wesson.pdf (Describing myriad vulnerabilities and only long-range possible defenses). Note Dr. Humphreys has made further response, which will be incorporated in next draft and posted in full for public access at SSRN or Google Docs.

[6] Dr. Humphreys, http://radionavlab.ae.utexas.edu/images/stories/files/papers/antiSpoofStraightTalk_Wesson.pdf.

[7] Telephone conference author hereof with {awaiting confirmation } dated 28 March 2012 and e-mail to author dated 29 March 2012, Former Electronic Warfare/Comsec Specialist, US Army Intelligence and Security Command, Director Product Management, Ericsson 1993-2000, Director Product Marketing, Tekelec 2000-2005, Director Strategic Market Research, Tekelec, 2005-2008.

[8] Michael Schearer, Experienced privacy, technology & digital rights researcher; founder of MyFreeState , the Freedom Report, and the Assault on Privacy, projects which document abuses of freedom, liberty, and privacy. Owner of Leverage Consulting & Associates , a computer security business. Spent nearly nine years in the United States Navy as an EA-6B Prowler Electronic Countermeasures Officer. Military experience includes aerial electronic combat missions over both Afghanistan and Iraq and nine months on the ground doing counter-IED work

Dr. Humphreys, stated, **[**i]f indeed localization is primarily GPS-based, then there is certainly a possibility that people will jam or spoof their phones to prevent or manipulate GPS tracking.[9] It is incumbent upon the government and the telecoms to inform the public of the safety and efficacy of these reforms, *before* their implementation places our public at risk.

2. The infiltration of law enforcement by the cartels/organized crime will place the public at severe risk of harm from abuses of warrantless access granted to virtually all public servants from the President down to as-yet undefined "delegees"

Sadly, the infiltration of Mexico's government and law enforcement at virtually all levels is so widely-known that it hardly requires citations in support. Many documented cases are discussed in Revista Proceso 1843.[10] If it is simply a matter of a narco, "serving" in a (false/infiltrated) position of law enforcement/government to obtain without warrant location data of potential victims. We can only extrapolate the excessive abuses that will result, in particular in states in which infiltration is deep and pervasive. I note here for the benefit of international readers not familiar with the crime/infiltration situation in Mexico – the narco/cartel crime problem, both generally and regarding infiltration, varies greatly from state to state and can change radically in very short periods of time. The State of Morelos, is a state whose government and police force is considered to be relatively free of corruption, with its Federal Police being commended,[11] whereas Mexico City, recently touted as having low cartel activity, is presently under horrific cartel seige.[12]

---

with the U.S. Army. I am graduate of Georgetown University's National Security Studies Program, the author of multiple books, and a frequent speaker at computer security conferences such as ShmooCon, DEFCON, HOPE, and other international conferences.

[9] E-mail Dr. Humphreys to author, citing [GSM World magazine] It discusses how GPS receivers can be blocked and manipulated by jamming and spoofing. "You may also find this paper useful", which discusses spoofing and defenses to it: Kyle Wesson, Daniel Shepard, and Todd Humphreys, Straight Talk on Anti-Spoofing Securing the Future of PNT, http://radionavlab.ae.utexas.edu/images/stories/files/papers/antiSpoofStraightTalk_Wesson.pdf GPS World Jan. 2012); Humphreys, The GPS Dot and its Discontents Privacy vs. GNSS Integrity, GNSS ("The need to protect ourselves from invasive tracking will motivate use of subversive tools such as GPS jammers and spoofers. A rise in the use of these illicit tools has the potential to wreak havoc on the «good» GPS receivers — those built into our critical systems and infrastructure. The result: A looming showdown between privacy and GPS integrity"), advance copy sent to me by Dr. Humphreys, now available at http://www.insidegnss.com/auto/marapr12-Humphreys.pdf, Inside GNSS (March/April 2012).

[10] Proceso 1843: Investigation Reveals How Los Zetas Operate Within Mexican Security, http://bit.ly/GOXGjh, 8 March 2012 ("The arrest of four members of the criminal organization "Los Zetas" has revealed that operations are not only performed, but overlapped by the Mexican Army, the Attorney General's Office (PGR), the Federal Bureau of Investigation (AFI) and the Federal Police (PF), as well as state and municipal police forces, both in Coahuila and Nuevo Leon.).

[11] Adame acknowledges the Federal Police, El Sol Cuernavaca, 30 December 2011 ("They have contributed to the safety of Morelos"), http://www.oem.com.mx/elsoldecuernavaca/notas/n2366485.htm.

[12] See, Video: drug war of the cartels in the metropolitan area with the City, Mundonarco 23 April 2012, http://www.mundonarco.com/.

3. The prior law's requirement of registering all user data as a prerequisite to purchase of a cell phone and that database's ready-availability on the black market, coupled with the new law's warrantless real-time warrantless geolocation tracking, equips criminals with unprecedented weapons of massive potential destruction, and places targets at unprecedented risks of harm

Under prior law, cell phone purchasers were required to register user data as a prerequisite to purchase of a cell phone. Commendably, this requirement has been eliminated by LeyGeolocalización MX, and the database is scheduled to be destroyed. Remarkably, however, IFAI itself does not even know the location of that database,[13] and copies of it are readily available for purchase.[14] This data, coupled with real-time geolocation data, will result in unprecedented enhancement of criminals' ability to target unsuspecting victims. For this reason too, the law will cause more harm than good. It makes extant potential victims—particularly high-value ones such as family members of wealthy citizens.

4. LeyGeolocalización MX is over-reaching and redundant for one of its primary intended purposes, to "inhibit the theft of mobile phones and their use for criminal purposes"

An expert contributor to this research has stated it quite clearly: this law is unnecessary to inhibit cell phone theft:

> *You can deter mobile handset theft simply by blocking stolen devices from registering on a network with what we call a "black list" application. With Tekelec's Equipment Identify Register (EIR) product, you can enter a device's International Mobile Equipment Identity (IMEI) into the product's "blacklist" to prevent its registration on the mobile network and the phone will simply never log onto any cellular network. The IMEI identifies the actual handset hardware, unlike the IMSI, MSISDN and SIM, which are subscriber specific. You can assign individual and/or ranges of IMEIs to white (allowed), black (blocked) or gray (track) lists, the latter being a very handy feature I am sure Mexican Law Enforcement or drug cartels would want to have. The EIR system simplifies IMEI screening by integrating fairly flexible database management and signaling functions making it easy for any carrier to block network access for any phone that's reported stolen. The database is queried using a standard MAP message to*

---

[13] IFAI to destroy Cofetel Renaut (National Register of Mobile Phone Users) ("For now, the authorities require the location of the base data and its size, so that the transparency institute is able to initiate the corresponding process in accordance with the law, said Jacqueline Preshard').
http://www.elfinanciero.com.mx/index.php?option=com_k2&view=item&id=10482:ifai-y-cofetel-destruir%C3%A1n-renaut&Itemid=26 (30 March 2012).
http://www.elfinanciero.com.mx/index.php?option=com_k2&view=item&id=10482:ifai-y-cofetel-destruir%C3%A1n-renaut&Itemid=26

[14] Renaut (National Register of Mobile Phone Users) Bid online at 500 pesos ("The user who is identified as shaka_345 @, with location in Chihuahua, 500 pesos ensures that databases are sent on DVD to your doorstep.") http://www.eluniversal.com.mx/nacion/178140mail.html 3 June 2010.

> *determine whether a particular handset may be used in the network and a phone not in the right list can't be used..*
>
> *Every network owned and controlled by Carlos Slim Helu, Telcel, America Moviles, you name it. . . I have to say that I'm suspicious of this law's purpose when a technical solution is readily available to that specific problem, even though the other issues are far more difficult to address.*[15]

LeyGeolocalización MX is over-reaching and redundant for one of its primary intended purposes—to inhibit cellphone theft. Less-intrusive technology already exists and is currently deployed.

5. The legislation violates the Constitutional rights of Mexican citizens

The Constitutional concerns of this law are being globally-discussed. The potential for aggravated/criminal circumvention of privacy is being widely commented upon.[16] An appeal to the Human Rights Commission to challenge the constitutionality of this law is being petitioned.[17]

I have said in numerous public forums (e.g. Facebook and Twitter), that if I believed this law—and its related technology—would solve Mexico's horrific crime problems, I would gladly give up my Constitutional rights to privacy. Extraordinary circumstances sometimes require of citizens extraordinary sacrifices. However this is not the right law, not in these circumstances in which Mexico sadly finds herself.

Aside from the practical considerations of this law, discussed above, it is incumbent upon elected officials to not violate the Constitutional rights of their people, particularly in the name of reforms that will not achieve their stated purposes and that will in fact place the public at greater risk of harm.

---

[15] Telephone conference with author (awaiting confirmation to release name) of 28 March 2012 and e-mail to author dated 29 March 2012, Former Electronic Warfare/Comsec Specialist, US Army Intelligence and Security Command, Director Product Management, Ericsson 1993-2000, Director Product Marketing, Tekelec 2000-2005, Director Strategic Market Research, Tekelec, 2005-2008. Further input expected.

[16] Once upon a time in Mexico…, PAUL BERNAL'S BLOG, Privacy, Human Rights, The Internet and more, http://paulbernal.wordpress.com/2012/03/19/once-upon-a-time-in-mexico/.; Digital rights scholar, Mexican Luis The (un) constitutionality of the # LeyGeolocalización http://www.humanrightsgeek.blogspot.mx/ (Originally posted 3 February 2012, update 1 March 2012); "BNA E-Commerce Law Report, ELECTRONIC SURVEILLANCE: MEXICAN GEOLOCATION SURVEILLANCE PLAN CHALLENGES TELCOS TO PROVIDE REAL TIME DATA, On Westlaw, 17 BNA ECLR 497, 2012 WL 746334 (B.N.A.)(14 March 2012) or 7-day free trial available here http://www.bna.com/electronic-commerce-law-p6796/ ; SoMe enVivo, *Social Media and Citizen Security in Mexico,* Ktitza Rodgriguez, Global Voices blogger (cited in SoMe) and @EFF https://www.eff.org/deeplinks/2012/03/mexico-adopts-surveillance-legislation (March 2, 2012).

[17] Full legal analysis: http://www.scribd.com/doc/89730592/Analisis-Juridico-LeyGeolocalizacion, petition: http://actuable.es/peticiones/pidele-la-cndh-presente-accion-inconstitucionalidad-vs .

Even in a best-case scenario, surveillance of GSM geolocation data is entirely too inaccurate, unreliable and easily circumvented/corrupted for the public to rely upon as a safety mechanism; infringement of human rights based on this inaccurate data is unreasonable and places public at even greater risk of harm.

For the foregoing reasons, I prevail upon the Supreme Court to overturn this legislation. I plea for the public that had input into and caused these reforms to be implemented in the first place, to return to the table with adequate technological input from scholars and industry, to redraft or simply abandon these efforts.

Respectfully submitted,

Lisa M. Brownlee, Esq.

IFAI RESPONSE TO EARLIER VERSION

GOOGLE TRANSLATION

I refer to your application lodged at the Institute on 12 April this year, through which it submitted to our consideration some observations on the so-called "Geolocation Act", which has been approved and published in the Official Journal of the Federation.

In this regard, it is clear that the aforementioned "Geolocation Act" actually consists of a series of reforms to various regulatory bodies. On April 18 of this was published in the Official Journal of the Federation, "Decree amending and repealing certain provisions of the Federal Code of Criminal Procedure, the Federal Criminal Code, the Federal Telecommunications Act of Law Establishing Minimum Standards for the Social Rehabilitation of Convicts and the General Law of National Public Security System, "hereinafter reform.

With regard to comments raised in your letter, the Institute has no power to make an assessment of the efficiency that may arise if in practice the laws are amended, in that sense, you can only issue a statement generally within the scope of authority of the Ministry of Protection of Personal Data, in particular as regards privacy and personal data protection.

Under this premise, it warns that "Law Geolocation" only impacts on the subject of personal data in an area that is restricted to specific cases refer to those cases involving organized crime, drug crimes, kidnapping, extortion or threats . This is because the power conferred upon the Attorney General's Office is limited to apply to licensees or permittees of the telecommunications service by a simple craft or electronic media, geographic location, in real time, of mobile communication equipment are related to criminal investigations in this area.

In this regard, the Institute, as part of their responsibilities in the field of protection of personal data, ensure that:

- It limits the use of such personal data and information provided by licensees and permittees for research purposes only ministerial.

- During the transfer of personal data and its guard, will observe the security measures.

- It meets the purpose and principles of proportionality to ensure that personal data to be exchanged are strictly necessary.

- They observe the obligation to maintain the confidentiality of the data that those responsible are held in compliance with the aforementioned reform, and not communicated to unauthorized persons.

Also, the Institute will provide all technical support for the protection of personal data is required in order

to assist with the authorities so as not to violate that right of citizenship.

Do not omit to state that the above are intended to provide guidance from the strictly technical standpoint, and does not prejudge the decisions that if the House of the Institute could take in this regard in the exercise of the powers have been granted.