Geospatial Health 6(2), 2012, pp. 157-159

Letter to the Editor

Geocoding-protected health information using online services may compromise patient privacy - Comments on "Evaluation of the positional difference between two common geocoding methods" by Duncan et al.

Dear Editor,

I was very excited to read the paper by Duncan et al. (2011), which described the locational accuracy and ease of geocoding address information using online geocoding services, published in *Geospatial Health*. The authors produced a very thorough analysis highlighting the practical utility of Batchgeo, and they promote it as a free and powerful resource for geocoding addresses. Unfortunately, they failed to recognize that the use of online geocoding services such as Batchgeo and ArcGIS Online World Geocoding Service (which were used in their study) may have inadvertently disclosed protected health information to an external organisation.

Location of residence is identifiable information. Passing address information to Batchgeo or other online geocoding services jeopardizes patient privacy because the information may be logged and stored in their data servers. Batchgeo's map data security and privacy policy states that they may record information such as your web request, Internet Protocol (IP) address, and the date and time of the transaction (2011). Static IP addresses are unique and identifiable, and many websites such as Batchgeo use cookies to track users for personalized marketing purposes. Therefore, it is possible for an online geocoding service provider to identify the organisation submitting the geocode request and attribute the list of addresses it processes. Furthermore, this information may be augmented with the date of the geocode request and the dataset in question may become reverse identifiable.

Recognizing the sensitivity of health and finance data, and the requirement to keep the information private and secured, ESRI (host of ArcGIS Online World Geocoding Service) recommends that geocoding of these data be performed using locally-stored reference street address datasets behind a secure firewall (2011). Online geocoding services should not be used for geocoding-protected health information because patient privacy may be compromised and the organisation may be in violation of privacy legislation.

The intent of this letter is not to embarrass the authors of the study, nor is it to vilify online geocoding services (or to suggest that they may have malicious intent to use the information that was inadvertently disclosed to them). Instead, public health practitioners and researchers should be aware that online geocoding services should not be used on sensitive and protected health datasets for the reasons stated above.

References

Batchgeo. "Map data security and privacy policy." Webpage visited December 13, 2009. http://batchgeo.com/features/security/ (accessed on 13 December 2011).

Duncan DT, Castro MC, Blossom JC, Bennett GG, Gortmaker SL, 2011. Evaluation of the positional difference between two common geocoding methods. Geospat Health 5, 265-273.

ESRI, 2009. New geocoding solutions provide many options. ArcNews Online. Spring 2009 http://www.esri.com/news/arcnews/spring09articles/new-geocoding.html (accessed on 13 December 2011).

Sunny Mak

Public Health Analytics, British Columbia Centre for Disease Control
655 West 12th Avenue, Vancouver, BC, V5Z 4R4, Canada
Tel. +1 604 707-2575; Fax +1 604 707-2516
E-mail: sunny.mak@bccdc.ca