SCHOLARS
STRATEGY NETWORK

The U.S. Government Must Protect Citizens from Geolocational Disinformation and Surveillance AI

Jeremy Crampton, George Washington University

Artificial intelligence (AI) is becoming more powerful and is more embedded in society than ever. Global governments are beginning to regulate these types of technology, and to balance benefits with potential harms. Yet while significant attention has been paid to reducing risk in the realms of health, finance, and privacy, policymakers have left one element largely unaddressed: geolocation data. This data—which provides information on the physical location of a person or device, like a smartphone—is powerful, sensitive, and highly valuable. AI procedures that are already being adopted to acquire, process, and automate spatial and locational data are a particular concern that call for swift action. But policymakers can simultaneously look to the future and work to ensure that we develop independent, trustworthy AI governance for geolocation by drawing on the hard-won knowledge of the spatial digital revolution of the past two decades. To realize the best outcomes on privacy, combatting disinformation, and deanonymization threats, policymakers must partner with geospatial domain experts rather than legislate around them.

The Current Regulatory Landscape

In 2023, privacy legislation protecting "sensitive information" has been passed in California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Florida. A significant number of these laws include a provision covering "precise geolocation." Data that qualify as indicating precise geolocation are limited to a radius of 1,750 feet around their subject, the equivalent of approximately 1/3rd of a mile—significant territory in a densely populated urban area, as this interactive map of healthcare facilities in Washington, DC shows. In Europe, the EU AI Act has prohibited the real-time collection of biometric data, such as occurs in facial recognition technology. Concurrently, U.S. legislators have become increasingly concerned about the risks of artificial intelligence, and the White House issued an Executive Order calling for new standards to prevent AI bias, threats, or misuse. In 2018 in *Carpenter v. United States*, the Supreme Court held that law enforcement agencies required a warrant to obtain location data from cell-phone towers; however, this data is imprecise, and law enforcement actors switched to using richer data sources not covered by the ruling (like app-based location data sourced directly from Google.) While these are welcome developments in the ongoing need to secure privacy, geolocation has certain unique risks that this legislation and the policymakers concerned with it have yet to address.

Risks

There are three main categories of risk for geolocation data governance: disinformation, surveillance, and anti-trust/concentration of market. **Disinformation** (e.g. fake maps and data, propaganda, etc.), bias, and discrimination raise issues of trustworthiness, privacy, and ethics. The concern for AI is not just low-quality knowledge, but low-quality learning, and low-quality meaning. For example, predictive policing—where data is analyzed to predict and intervene on potential future crime—may be based on poor, false, or biased data that can lead to real-world discriminatory consequences.

- Fake data can infiltrate maps (spatial databases), intentionally or not. Fake data could be included in driving apps or autonomous vehicles to chaotic effect; AI could be applied to geospatial data in a manner that misclassifies satellite imagery.
- Disinformation may include falsely showing a person to be at a location when they were not—known as "location spoofing"—for blackmail or to cause reputational damage. "Deepfake geography" involves faking that a person is not at a place they should be: imagine truckers' data hacked to falsely show them as having deviated from their routes.
- Inadvertent misinformation proliferated by lack of relevant geospatial analytic expertise can lead to detrimental outcomes. Inaccuracy and uncertainty can arise from analyzing a phenomenon at the

wrong spatial scale (known as the "the Openshaw Effect"), or not accounting for how boundaries influence the scale of the analysis of aggregated data (referred to as "modifiable areal unit problem" or MAUP).

Surveillance and locational tracking, which can include wide-scale biometric identification in real time or upon review of previously gathered data, poses many threats to privacy. Inference of personally identifiable information based on geospatial data obtained through surveillance is all too easy, and can include privacy infringements like re-constituting encrypted data (deanonymization) and uncovering the identity of a person or organization that has been obscured (re-identification.) One well-known 2013 study found that knowing just four location points was enough to re-identify 95% of individuals, and that even when geospatial data is less precise, it can still reliable re-identify individuals—it takes a high factor of imprecision before location data loses its power to pinpoint. A new study of metro card travel data confirmed the findings that three random location points from within a period between one minute and one hour are sufficient to identify 67-90% of users. And facial recognition technology, which has many clear privacy risks, is now widely employed by law enforcement.

The limits of **anti-trust regulation and market concentration** among tech companies point to increased opportunities for large data breaches or unethical use. The market is dominated by deep-pocketed AI tech companies including OpenAI, Google, and Microsoft; these companies own and control the high-tech market, especially "high compute" fields like machine learning and AI training, effectively locking out competitors.

Recommendation to Begin Risk Mitigation

The Offices of Science and Technology Policy (OSTP) at the White House and Congress can hold hearings with geospatial industry and academic experts to identify current and emerging threats to privacy from geolocation data and geolocation services and analytics. The quality and efficacy of legislation will depend on collaboration with and transparency from the experts who are designing and deploying these emerging technologies