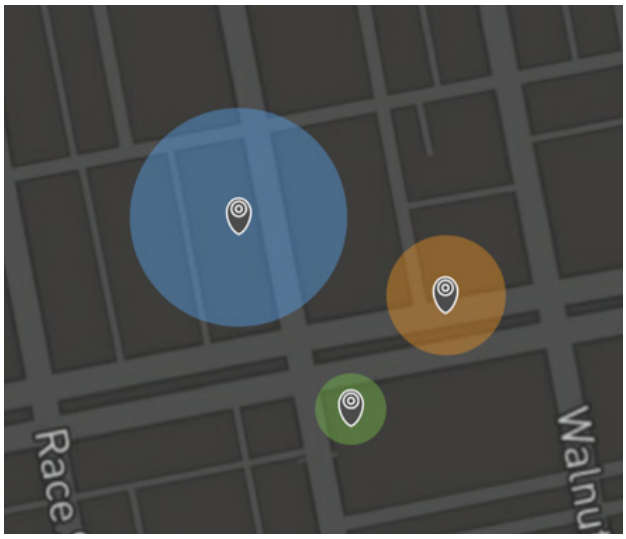
# The Geointelligence Revolution

## Real-Time Reconnaissance and Its Dangers

Alexander | Nocks



*Brief No. 10.5*

P | I | P | S

*The Project on International Peace and Security*
Institute for the Theory and Practice of International Relations
The College of William and Mary

Please direct inquiries to:
The Project on International Peace and Security (PIPS)
Institute for the Theory and Practice of International Relations
The College of William and Mary
427 Scotland Street
Williamsburg, Virginia 23185

tele. 757.221.1441
fax. 757.221.4650
pips@wm.edu

Electronic copies of this report are available at: www.wm.edu/pips

# The Geointelligence Revolution
## Real-Time Reconnaissance and Its Dangers

APRIL 2018

Alexander Nocks

P|I|P|S *The Project on International Peace and Security*
Institute for the Theory and Practice of International Relations
The College of William and Mary

# The Geointelligence Revolution
## Real-Time Reconnaissance and Its Dangers

*Actors—from lone-wolf terrorists to transnational criminal organizations—will soon have geospatial intelligence capabilities currently limited to states. In the next five to ten years, increasingly accessible geospatial data will allow adversaries to conduct remote, real-time reconnaissance with minimal risk of detection. Improvements in commercial satellite imagery, paired with an increase in publicly-available, geolocated data, will empower non-state actors at each stage of the attack cycle. U.S. policymakers must prepare for a future in which the exploitation of open-access data is a constant threat.*

## Introduction

Publicly available geospatial information and aerial imagery are increasingly satisfying the reconnaissance needs of terrorist organizations and other non-state actors. As private companies compete to convert raw inputs into actionable intelligence and sell their ever-growing stocks of data, non-state actors will have access to geospatial intelligence capabilities that were previously limited to states. Reconnaissance that once required risky, time-intensive, in-person investigation will be carried out instantaneously and remotely. These new geospatial intelligence abilities empower non-state actors throughout the attack cycle—target selection, attack planning, and attack execution—while simultaneously reducing the ability of states to detect such attacks before they occur.[1]

Non-state actors will benefit as developing technology improves the low-level geospatial intelligence abilities that they have adopted over the past 13 years. Anticipating rapid improvements in public geospatial intelligence capabilities, the U.S. government must prepare to detect and counter attacks by non-state actors exploiting real-time remote reconnaissance.

## Dual-Use Dilemma

> *"Technology...is a queer thing; it brings you great gifts with one hand and it stabs you in the back with the other."*
>
> – C. Snow[2]

Geospatial intelligence (GEOINT) is the process of deriving intelligence from geospatial information and aerial imagery.[3] When analyzed, these inputs provide significant situational awareness by allowing remote actors to describe, assess, and model physical features and geographically referenced activities. The public GEOINT field is growing as actors take advantage of emerging GEOINT inputs and analysis abilities.

There is an inherent tension between the constructive and destructive applications of GEOINT. This dual-use dilemma—in which the same information can be used to advance conflicting ends—has gone largely unaddressed by the policy community.[4] Since low-level GEOINT currently available to the public introduces relatively few risks for national security, the benefits of public GEOINT have overshadowed its dangers. Mapping storm damage saves the lives of evacuees—but it may also direct looters to vulnerable areas. Improvements in public GEOINT capabilities will enhance both sides of the dual-use dilemma.

*Dual-Use Dilemma Case Study: Fitness-tracking Devices*

Data derived from location-enabled fitness trackers highlights the dual-use dilemma. Many users of fitness trackers focus on the personal utility of sharing their workout activity but doing so also disseminates revealing geospatial information. Widespread adoption of these devices increases the risk posed by making the data they collect publicly available.

One tracking company, *Strava*, demonstrates the conflicting uses of the same geospatial information. While *Strava's* publicly available aggregated data provide unique traffic insights to city planners, they also inadvertently reveal sensitive information about U.S. military and intelligence activities.[5] This "social media for athletes" tracks, sells, and displays users' aggregated location data in a heatmap.[6] Users have willingly shared their data with the company, often without realizing that it will be shared with others.

Publicly available personal location information, such as the data collected and shared by *Strava*, can be exploited to harm U.S. security in three significant ways.

- *Locating Secret Facilities.* While covert bases can be difficult to find with commercial satellite imagery, the *Strava* heatmap inadvertently revealed several remote facilities.[7] Many forward operating bases in Helmand province, Afghanistan, including some not readily visible on commercial satellite imagery, stood out on the heatmap.[8]

- *Mapping Activity within Facilities.* The *Strava* heatmap also revealed routines of life within and around the facilities it exposed. Aggregated patterns of movement exposed transportation routes, internal base layouts, and concentrated activity within military bases that revealed potential targets—where troops live, eat, or work.

- *Tracking Personal Behavior.* When users failed to navigate *Strava's* default privacy settings, the app revealed their personal locations and identifying information with the public.[9] S*trava* shares identifying information on public leaderboards, with users who cross each other's paths, and among users participating in a given challenge.[10] For example, the leaderboard for a 600 meter stretch outside an airbase in Afghanistan included the full names of over fifty service members who ran it.[11] Similarly, the leaderboard of a seven kilometer loop around the runway at Djibouti's Chabelley Airfield reveals the names of several runners who completed the route, and even that one of those users was transferred to an airbase in Germany in 2016.[12]

The dual-use dilemma applies to not only location-tracking data but also other GEOINT inputs. The growing volume and quality of publicly accessible geospatial information and aerial imagery will make GEOINT more useful for all actors. Demand for improved public GEOINT abilities is inadvertently creating an overlooked opportunity for potential U.S. adversaries.

## Democratization of GEOINT

> *"The demand, the drive, the ability for geospatial information to really be the basis for everything that almost everyone does is what the future's going to be."*
>
> –J. Goolgasian[13]

Policy and technological barriers have previously denied non-state actors access to valuable geospatial information and aerial imagery. Until recently, only states could collect and—at their discretion—distribute key GEOINT inputs. However, the United States has slowly deregulated geospatial industries over the past three decades, allowing companies to provide low-grade GEOINT abilities to the public.

### *Geospatial Intelligence Goes Public*

Conducting public GEOINT was impossible until the late 20th century since states completely controlled the requisite inputs. Potentially sensitive GEOINT inputs reached the public only when the government chose to declassify it.[14] While restricting access to GEOINT inputs was an effective method of mitigating the risks posed by the data, it also stunted commercial growth.[15]

The United States passed the Land Remote Sensing Policy Act of 1992 to open the satellite imagery market to private companies in response to the demands of the scientific community and previous failures to commercialize.[16] Similarly, in 2000, the United States ended its use of Selective Availability—the intentional degradation of civilian Global Positioning System (GPS) signals—to make commercial GPS more viable.[17] Again, commercial benefits were cited to justify the policy change.[18]

### *Widespread Low-Grade, Public Geospatial Intelligence*

Businesses quickly entered the new public GEOINT market, providing consumers with early location-tracking devices (such as GPS units), free online maps, and aerial imagery.[19] This low-grade GEOINT quickly became ubiquitous, despite its limited accessibility, granularity, and temporal resolution.

Existing public GEOINT has been adopted primarily by four groups.

- *Individuals.* Data processed by location-enabled apps, coupled with contextualizing aerial imagery have redefined human mobility. Online maps that provide navigation directions

for a given environment allow users to operate like locals in foreign settings. Adding geospatial information to these maps further enhances their utility. For example, Four-Square—a location-based social network—shows the location of popular establishments and special offers based on users' location history.[20] More sophisticated applications display activity—like crowd sizes and bus movements—in real time.[21]

- *Businesses.* Companies use public GEOINT to connect with consumers, analyze market dynamics, and monitor equipment. Understanding customer movement has unlocked a new field of location-based marketing. For example, geofencing allows companies to send notifications to their apps' users when they are within a certain distance of the store.[22]

  Additionally, companies have come to rely on aerial imagery for corporate reconnaissance and monitoring business infrastructure. For example, in 2010, UBS Investment Research found that studying satellite pictures of Walmart's parking lots to estimate customer footfall was more effective at predicting quarterly earnings than traditional methods.[23] Furthermore, aerial imagery abilities are quickly replacing in-person monitoring of critical infrastructure. Instead of flying over a pipeline to check for damage daily, automated analysis of aerial imagery will instantly notify the company when something goes wrong. Soon, this aerial imagery analysis ability will extend to tracking delivery trucks in near-real time.[24]

- *Non-Governmental Organizations (NGOs).* Public GEOINT enables humanitarian organizations to monitor for human rights violations and facilitate disaster relief efforts around the world. [25] Commercial satellite imagery has revealed torched Rohingya villages in Burma,[26] reeducation camps in the Democratic People's Republic of Korea,[27] and mass graves in Burundi.[28] Analyzing commercial aerial imagery enables humanitarian organizations to identify atrocities that would otherwise have gone unnoticed and even predict atrocities before they occur.[29]

  To help victims and responders during humanitarian crises, NGOs use GEOINT to create online crisis maps—continuously updated, crowdsourced maps—to show damage and recovery efforts.[30] By overlaying geospatial data reported by the those affected on detailed maps and three-dimensional models, analysis groups provide actionable insights to organizations on the ground.[31]

- *The U.S. Government*. Since public GEOINT is often less expensive and offers unique insights not provided by classified alternatives, it is quickly becoming an integral part of the National Geospatial-Intelligence Agency's (NGA) intelligence operations.[32] For example, Open Street Map aggregates locals' knowledge, providing an otherwise unachievable level of granularity. By synthesizing public and classified GEOINT inputs, the NGA can deliver more comprehensive insights.

  The U.S. government increasingly relies on commercial analysis. The xView Detection Challenge is indicative of this shift.[33] This open contest, recently launched by the Defense Innovation Unit Experimental (DIUx) and the NGA, harnesses public talent to advance the government's GEOINT capabilities. Contestants use annotated satellite imagery from

> DIUx to design algorithms that identify objects of interest for disaster relief operations.[34] New and existing algorithms are critical to utilizing the growing abundance of aerial imagery and geospatial data produced each day. Integrating commercial data and analysis allows the NGA to capitalize on cutting-edge private development and offer its customers the best insights as quickly as possible.[35]

These stakeholders—including the NGA—are working to improve public GEOINT capabilities and would be significantly disadvantaged by further restrictions on geospatial information and aerial imagery.[36]

*Future Access to High-Grade Geospatial Intelligence for the Public*

As publicly available geospatial information and aerial imagery grow in volume and quality, current users of low-grade public GEOINT will soon have significantly improved capabilities. The clear profitability of collecting, analyzing, and distributing GEOINT inputs is leading more organizations to enter the public GEOINT market.[37] These companies will satisfy the growing demand for public GEOINT improvements by providing better inputs and more actionable analysis.

## Improving Public Geospatial Intelligence

> *"A kid in Africa with a smartphone has access to more information [today] than the president of the United States did 15 years ago."*
>
> – R. Kurzweil, 2012[38]

Today, demand for increased public access to enhanced GEOINT drives technological developments that will increase the volume, granularity, and temporal resolution of publicly available GEOINT inputs. These developments—including improved crowdsourcing, which turns large segments of the population into geolocated sensors and miniaturizing aerial imagery technology—will significantly improve public GEOINT abilities in the next five to ten years.

*Improving Geospatial Information*

Expanding mobile device usage and internet connectivity, along with emergence of the internet of things, allows more real-time geospatial information to be collected at a more granular level. These trends improve crowdsourcing—the delegation of data collection or analysis to a wide, largely uncredentialled community. Regulating these communities is especially difficult, because it is impossible to know what they will create.[39] With internet and location-tracking device usage increasing, the size of the crowd producing location-based data grows.[40]

Two primary developments are driving the improvement in geospatial information available to the public.

- *Rise of Volunteered Geographic Information* (VGI). Volunteered geographic information is location-based, user-generated content—information users choose to share with the world. People share their location for social gain, in-app rewards, or to enjoy personalized, location-based special offers and experiences. As more of the public can easily report location data, the variety of VGI being collected is quickly expanding beyond traditional geotagging. For example, users report police activity and locations through crowdsourcing apps like *DUI Dodger*, *Buzzed*, and *Checkpoint Wingman*. These apps display interactive, real-time maps of officer locations and notify users when checkpoints are moved or established, helping users avoid arrest.[41] During the 2011 London riots, the app *Sukey* created an interactive crowdsourced map showing where riot police were and provided an interactive compass to steer users away from the police. The information was collected by users photographing riot police and uploading geotagged images to a central map.[42]

  Between the status-driven social media scene and ubiquity of location-dependent apps, location-sharing has become commonplace. The growing pressure to "check-in" at hot spots encourages users to share their location and demand easier ways to do so. Comfort with location sharing for social purposes makes individuals more susceptible to the misuse of their data through location-based technologies.

- *Growth in Ambient Geographic Information (AGI).* Ambient geographic information refers to location-based information shared passively, for example, the sale of cellphone tracking data that a user inadvertently produces. By connecting more devices, the internet of things creates more ambient geographic information.[43] These personal trackers—including insulin pumps, fitness trackers, and connected cars—map the world at a more granular level than ever before.

  With nearly five billion smartphones globally, a significant portion of the world is constantly connected to location-aware computers.[44] Continuous tracking has become the norm, providing widespread, real-time AGI. Many applications depend on tracking users' locations; over 75 percent of all Android apps track users' location.[45] For example, dating apps harness location data to better connect users. Other apps that offer augmented reality experiences—in which a geolocated device enhances the physical reality with additional features on the screen—introduce a new range of user experiences dependent on tracking users' locations.[46] Constantly providing one's location, and the loss of privacy it entails, is becoming an acceptable cost of doing business in the social marketplace.

In an era of ubiquitous smart devices, individuals' movements across space and time are continuously recorded, creating a large stream of data for analysis. Crowdsourcing developments will further expand the stock of publicly available geospatial information. Mobile data collection is already making information that would have taken months to assemble accessible in just two weeks.[47]

*Improving Aerial Imagery*

Aerial imagery contextualizes geospatial information, while also offering unique insights of its own. With remote sensing technology becoming more affordable, smaller, and easier to produce, many companies are entering the aerial imagery market, equipping the public with new GEOINT inputs that will soon offer high spatio-temporal resolution coverage of much of the planet.

Two trends are primarily driving improvements in publicly available aerial imagery:

- *Proliferation of Unmanned Aerial Vehicles (UAVs).* Unmanned aerial vehicles are becoming increasingly capable and inexpensive. These low-flying, short-ranged systems are accessible via personal ownership or companies selling surveillance services. UAVs can deliver images with resolutions of one inch within hours, while others offer real-time video footage.[48] By 2025, total commercial UAV sales are expected to exceed 90 million units.[49]

- *Development of Small Satellites (Smallsats).* Lighter, smaller, and easier to build than traditional satellites, smallsats have lower production costs and shorter production times. This streamlined production allows private companies to launch more satellites, making higher revisit rates and even full constellations across low Earth orbit attainable.[50] As they become less expensive, smallsat constellations will be able to provide a real-time view anywhere in the world on short notice.

Smallsat and UAV growth allows more aerial imagery to be collected and continuously updated for less money. The explosion in data is moving the aerial imagery field towards enabling anyone to conduct real-time reconnaissance on short notice anywhere in the world.

*New Gatekeeper: Data Brokerage Companies*

While technological developments allow an unprecedented volume of GEOINT inputs to be collected, much of that data must pass through brokerage companies before a potential adversary can use it. These companies act as information chokepoints—aggregating data, repackaging it for distribution, and oftentimes converting the inputs into actionable insights.

There are two primary types of companies that connect users to the growing potential of public GEOINT:

- *Data Brokerage Companies.* In their simplest forms, data brokerage companies collect data from the public—often including geospatial and identifying information—and sell it to third parties. For example, *Strava* recently launched a brokerage operation, Strava Metro, that sells its users' spatio-temporal tracking data to urban planners who use for analyzing general traffic patterns and predicting future activity.[51]

  With improvements in predictive analytics, geospatial information and analysis will become more valuable. While the information is usually sold without personal

identification, the uniqueness of each person's movements makes it possible to match ostensibly anonymous tracking records to their creators.[52] Some businesses are already using individuals' routines to forecast their future location and provide location-based, just-in-time offers.

- *Aerial Imagery Analysis Companies.* Many new analysis companies are providing customers access to both raw and analyzed aerial imagery. Their business model rests on converting aerial imagery into actionable intelligence for the public. These companies provide a range of products, including detailed, three-dimensional maps for planning in urban areas and downloadable, editable maps that provide a common operating picture offline.[53]

  As satellite companies like Planet, DigitalGlobe, and Astro Digital produce a growing volume of aerial imagery, startups like Descartes Labs, which claims to be "the missing link in making satellite imagery useful," are aggregating, cleaning, and reselling data from the crowded field of satellite imagery producers.[54] Others, like Orbital Insight, simplify the process by providing deliverables that directly answer customers' questions.[55] This rapidly growing field allows anyone to take advantage of the improvements in aerial imagery.

Without the services of data brokerage and aerial imagery analysis companies, many of the anticipated uses of public GEOINT would be unattainable. Technological developments expand these companies' offerings, significantly increasing their influence. As these companies provide enhanced GEOINT inputs and analysis to the public, they are also inadvertently equipping potential adversaries to conduct more effective attacks.

## Evolving Threat: Emergence of Real-Time Reconnaissance

> *"Our technological powers increase, but the side effects and potential hazards also escalate."*
>
> – A. Toffler[56]

The United States' adversaries have used public GEOINT alongside in-person reconnaissance to prepare for attacks, but technological developments will soon render in-person reconnaissance unnecessary. As public GEOINT offers closer to real-time insights, it will shift from complementing in-person reconnaissance to offering superior insights—not only for target selection and attack planning, but also for attack execution. This new era of higher-quality public GEOINT will increase the risk posed to the United States by adversaries with access to real-time reconnaissance.

### *Current Threat Assessment: Low-Grade Public Geospatial Intelligence*

Although current public GEOINT capabilities rely on outdated aerial imagery and intermittent geospatial information, internet reconnaissance has become commonplace in attack cycles.[57] Criminal networks, terrorist organizations, and other non-state actors have been quick to employ

low-grade public GEOINT capabilities, primarily via Google Earth and geotagging on social media.[58]

Access to low-grade public GEOINT has improved two phases of the attack cycle:

- *Target Selection*. Location data is automatically embedded in the metadata of most photos taken on a cellphone. When a picture is uploaded to social media, connected users can see where that person was when the picture was taken. Connecting a photo subject and photographer to a given location makes targeting information public. Geotagging reveals sensitive information by sharing the specific locations of potential targets. Most users are not aware of the threat posed by geotagging, nor do they realize when they are publishing geotagged information.[59] Nonetheless, savvy actors know that exploiting geotagged information can create actionable insights.

  Revealing the exact coordinates of targets greatly increases the odds of their destruction.[60] When a fleet of helicopters arrived at an unidentified base in Iraq in 2007, U.S. soldiers uploaded pictures to Facebook that revealed their location.[61] Insurgents then used the photos' coordinates to launch precision mortar strikes, significantly damaging four of the new Apaches.[62] Geotagged photos have also led to active shelling of Ukrainian soldiers. These soldiers admitted to looking through Russian and separatist social media accounts to determine their locations as well.[63]

- *Attack Planning*. Google Earth provided non-state actors aggregated satellite imagery of most of the planet for the first time. While it lacks the granularity and temporal resolution needed to be as dangerous as many feared, it still revolutionized attack preparation by allowing actors to observe spatial relationships, plan attack routes, and identify a target's vulnerabilities.[64]

  Investigating planned attacks frequently reveals Google Earth reconnaissance, including a 2007 plan to blow up fuel tanks at New York's John F. Kennedy airport.[65] Satellite imagery allowed the would-be attackers to locate the fuel tanks easily, quickly, and remotely. In 2016, assailants studied Google Maps in preparation for an attack on India's Pathankot Airbase that killed more than ten people.[66] The information they used included high resolution satellite imagery and geospatial information crowdsourced from locals who mapped on-the-ground data as part of Google's mapathon contest.[67] Seeing that forests surrounded the base made the terrorists confident that the attack would be "easy."[68] Likewise, in preparing for the devastating 2008 Mumbai attacks that killed 166 people, Lashkar-e-Taiba made extensive use of internet reconnaissance. Handlers and strategists searched for and selected targets from Wikimapia and other internet services and provided Google Earth imagery to the assailants, who were then able to easily recognize and navigate to their targets.[69] However, Google Earth provided only incomplete reconnaissance; Lashkar-e-Taiba also made several planning trips to Mumbai.[70]

While states maintain a GEOINT comparative advantage with higher resolution and more frequently updated aerial imagery, terrorist organizations have fewer needs. Remote surveillance of any kind facilitates attacks by lowering costs, risk of detection, and often offering better

intelligence than could be gathered in person. Nonetheless, satellite imagery thus far has been unable to replace the insights delivered by in-person reconnaissance.

*New Threat: Real-Time Remote Reconnaissance*

The next phase of public GEOINT abilities is real-time remote reconnaissance, in which potential adversaries can remotely conduct all surveillance required to prepare for an attack from a laptop. Real-time remote reconnaissance is less expensive, harder to detect, and faster than traditional reconnaissance methods. It allows central agents to easily conduct reconnaissance, planning attacks for others without exposing themselves to detection. The improving spatio-temporal resolution of geospatial information and aerial imagery will soon make this scenario the norm, allowing potential attackers to completely forgo in-person reconnaissance—currently a key opportunity to detect attacks before they occur.

The combination of local-level knowledge with aerial surveillance allows potential adversaries to see around physical obstacles and gain enhanced situational awareness throughout three general phases of the attack cycle.

- *Target Selection*. Improved public GEOINT abilities reveal vulnerabilities that would otherwise be difficult to detect. Understanding physical environments, defensive structures, and security operations facilitates sophisticated target selection. This knowledge allows planners to compare vulnerabilities across a wider array of potential targets more quickly and easily than in-person reconnaissance would allow.

- *Attack Planning*. Real-time remote reconnaissance facilitates attack planning more effectively than either on-site reconnaissance or asynchronous remote reconnaissance. Visualizing the minutia of an operating environment enables attackers to prepare escape routes, plan for contingencies, and otherwise develop knowledge approaching that of a local.[71] Public GEOINT will provide detailed insights allowing attackers to make precise plans without risking in-person detection.

- *Attack Execution*. By showing attackers and their handlers where responders, victims, and other entities are as an attack unfolds, real-time remote reconnaissance will provide attackers unprecedented situational awareness.[72] Knowing how the environment is changing will help assailants inflict greater damage and escape more easily. Attackers have used live television to track responses in real-time, but that method offers a more incomplete and avoidable picture. For example, Lashkar-e-Taiba handlers watched news accounts of the 2008 Mumbai attacks on television to learn about the movement of security forces.[73] Real-time reconnaissance, including live aerial imagery, will provide more holistic and reliable situational awareness.

Improving public GEOINT enhances potential adversaries' abilities throughout the attack cycle. Real-time remote reconnaissance better equips non-state actors to plan attacks, evade detection, and inflict greater harm. As technology continues to develop, the real-time reconnaissance era will be the new reality.

## A Counter-GEOINT Future

*"When everything is connected, nothing can be hidden."*

– M. Goodman[74]

The United States has restricted access to satellite imagery to protect potential targets from GEOINT reconnaissance—a policy approach known as "prior restraint." Improvements in public GEOINT renders those policies insufficient and untenable. Prohibiting access to certain types of satellite imagery does not address the vulnerabilities that public geospatial information reveals, and the growing volume and usefulness of satellite imagery makes denying access costlier.

Instead the United States should prepare for counter-GEOINT operations to address the imminent democratization of high-level GEOINT abilities. As the real-time remote reconnaissance era will allow potential adversaries to prepare attacks without in-person surveillance, it is imperative to develop alternative detection methods. The NGA has acknowledged the need for counter-GEOINT policy but has not publicly offered any specifics.[75]

### *Shortcomings of Prior Restraint Policy*

Current prior restraint policies seek to mitigate the dangers of public GEOINT by denying some users access to certain subsets of satellite imagery. Each U.S. remote sensing company's operations license is contingent upon their compliance with international obligations[76] and U.S. national security policy.[77] Compliance requirements take two basic forms—they limit either acquiring or disseminating certain satellite imagery. To protect national security, statutory restrictions additionally limit the spatial resolution of satellite imagery, prohibit collection on select sensitive sites,[78] and bar selling satellite imagery to certain buyers.[79]

Current regulations include two main exceptions that allow the government to censor satellite imagery beyond baseline licensing restrictions.

- *Emergency Shutter Control*. When national security, international obligations, or foreign policies are at risk, the Secretary of Commerce may require satellite imagery companies to further limit their collection or dissemination of certain images.[80] This controversial policy has never been implemented.

- *Checkbook Shutter Control*.[81] The U.S. government can buy exclusive rights to all the satellite imagery it seeks to remove from the market.[82] Before entering Afghanistan in 2001, the Pentagon bought all available commercial satellite imagery of the region, denying anyone else access for the first three months of the war.[83] As more companies are producing more satellite imagery, buying out the entire market for a given region is becoming more expensive.[84]

Three primary flaws are making meaningful prior restraint policy unachievable.

- *Significant Costs to Other Users.* Denying access to GEOINT inputs hurts the many humanitarian, social, and commercial enterprises that also rely on public GEOINT. With commercial satellite imagery playing a growing role in their operations, the costs of denying access are rising. As access to real-time satellite imagery becomes the norm, attempts to delay the release of certain images may undercut their usefulness. These costs will continue to rise as commercial satellite imagery plays a bigger role

- *Alternatives to Regulated Satellite Imagery.* Foreign entities provide satellite imagery that is banned in the United States.[85] While many top satellite imagery companies are currently U.S.-based, the market is going global. Furthermore, geospatial information and aerial imagery from UAVs reveal the same vulnerabilities as would satellite imagery.[86] Reducing the satellite imagery's quality has little effect when the same information can be readily acquired elsewhere.[87]

- *Undermines U.S. Satellite Imagery Market.* Requiring U.S. companies to degrade their satellite imagery reduces their ability to compete and creates a profit-incentive for companies to move overseas where the United States has less regulatory control. Restrictions that drive U.S. companies to offshore makes prior restraint a self-defeating policy.

Data restrictions undercut the many constructive uses of satellite imagery, fail to deny potential adversaries significant GEOINT insights, and drive satellite imagery companies overseas. Current prior restraint policies can no longer be relied on to defend the United States against the dangers presented by potential adversaries using public GEOINT.

*Counter-GEOINT Solution*

The challenge of regulating dual-use information is balancing its constructive and destructive potential. However, the high risks of public GEOINT do not necessarily mean that they outweigh the benefits. Instead of denying all users access, the United States should pursue strategies to mitigate the risks, while maintaining the benefits of public GEOINT. Many of public GEOINT's most significant destructive applications involve soft, civilian targets; the growing utility of high-level, public GEOINT in those areas makes restricting access too costly.

Nonetheless, the threats enabled by public GEOINT abilities are too significant to go unmonitored. Data brokerage and imagery analysis—which for now are predominantly U.S.-based—distribute potentially dangerous GEOINT. These information chokepoints are the only way to access the most advanced public GEOINT capabilities. Prohibiting companies from operating will force them abroad and beyond the reach of future U.S. regulations. Rather than limiting their operations, the United States should monitor them. As pre-attack reconnaissance moves entirely online, reconnaissance detection efforts must do so as well.

Three general strategies can best lessen the risks from public GEOINT without undermining its benefits.

- *Precise Restrictions.* For highly-sensitive sites—such as military bases—the destructive potential of sharing GEOINT inputs outweighs its benefits. Those facilities can best be protected by denying any form of surveillance. Imposing legal shutter control on domestic companies and checkbook shutter control on foreign companies can minimize the dangerous aerial imagery available. These sites should also block location tracking on their premises by prohibiting location information sharing and using jammers to make location tracking impossible.[88]

- *Mandatory Reporting.* All U.S. companies should be required to report the sale of geospatial information, aerial imagery, or GEOINT analysis. By collecting buyer and data subject information, the United States can detect remote reconnaissance as it happens. Since many companies offer specialized data and analysis, the best reconnaissance will likely include multiple purchases from different companies. Aggregating purchase data will reveal where reconnaissance is being targeted. Analyzing those patterns can reveal potential plots and establish investigation subjects, thereby allowing attacks to be detected before they occur.

- *International GEOINT Agreement.* While most public GEOINT is currently facilitated by U.S. companies, GEOINT companies are proliferating worldwide. To ensure continued security as the market diversifies beyond the reach of U.S. regulations, the United States should work with the international community to coordinate policies for selling GEOINT inputs. Doing so will create a more comprehensive and reliable monitoring network, enabling plots to be detected even when potential adversaries buy GEOINT products from companies in different countries. While there are instances in which states will assist non-state actors' GEOINT operations, in most cases public GEOINT's dangers affect all states.

Prior restraint and other blanket GEOINT denial programs are too clumsy for the future public GEOINT market. They undermine too many benefits of public GEOINT, while failing to address too many dangers. For example, U.S. regulations forced satellite imagery company DigitalGlobe to degrade the wild fire imagery it provided to the Alberta Provincial Government. Regulations required that nearly three-fourths of the data be discarded, needlessly limiting the insights provided to the firefighters.[89]

## Conclusion

> *"Without location, there is no context."*
>
> – C. Fake[90]

Terrorist organizations and other asymmetric actors regularly use the best GEOINT capabilities available. While the initial democratization of GEOINT led to its use in planning many attacks, technological improvements that make far more current and granular GEOINT inputs available to the public will significantly increase the threat enabled by public GEOINT. The combined shift towards increased granularity and temporal resolution of crowdsourced geospatial information, aerial imagery, and automated analysis accessible to the public will allow non-state actors to

remotely conduct real-time reconnaissance within the next five to ten years. If unaddressed, this GEOINT upgrade will make attacks more dangerous, easier to plan, and harder to detect.

The real-time reconnaissance era emerging in the next five to ten years is just the beginning. Public GEOINT will continue improving. What is exclusively the domain of states today will be proprietary tomorrow. What is proprietary today will be open source tomorrow. Open source resources already can match many of the core capabilities of key industry players.[91] For now, the most threatening capabilities are sold, not open access, making monitoring data sales an effective means of tracking potentially threatening GEOINT operations. By adopting counter-GEOINT monitoring practices and encouraging their standardization worldwide, the United States can maximize the utility and mitigate the dangers of improving public GEOINT.

[1] In-person reconnaissance is one of the most vulnerable parts of attack planning, so removing it makes planning attacks much less risky.
[2] Marc Goodman, *Future Crimes* (New York: Doubleday, 2015), 7.
[3] Colin Clark, "Cardillo: 1 Million Times More GEOINT Data In 5 Years," *Breaking Defense* (blog), June 5, 2017, https://breakingdefense.com/2017/06/cardillo-1-million-times-more-geoint-data-in-5-years/.
[4] Michael J. Selgelid, "Governance of Dual-Use Research: An Ethical Dilemma," WHO, June 30, 2009, http://www.who.int/bulletin/volumes/87/9/08-051383/en/.
[5] For example, some users reported theft after their public workout routes led to storage facilities on their property. See "Fitness Dystopia in the Age of Self-Surveillance," accessed February 5, 2018, https://www.bankinfosecurity.com/blogs/fitness-dystopia-in-age-self-surveillance-p-2590.
[6] *Strava's* website and mobile apps connect millions of athletes, allowing them to compete against themselves, their neighbors, and enthusiasts around the world. Using a smartphone or other GPS enabled device—like smart watches or Fitbits—*Strava* collects numerous performance metrics including route and time. *Strava* displays a portion of the aggregated location data in a publicly available heatmap and sells even more data.
[7] The *Strava* heatmap allowed third parties to discover these sensitive locations faster.
[8] Alex Hern, "Fitness Tracking App Strava Gives Away Location of Secret US Army Bases," The Guardian, January 28, 2018, http://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.
[9] *Strava's* website allows users to upload GPS segments—short portions of a given workout route that can be compared across users. Anyone can upload a fake segment, mimicking real exercise anywhere in the world. Once uploaded, the segment reveals information shared by the overall top ten per gender and age group for that segment including when they ran, who they ran with, and, depending on privacy settings, where else they have run. While *Strava* eventually changed its privacy policies, failing to discover the opt-out options—as many users did—revealed undesirable levels of information to virtually anyone. See Steve Loughran, "Advanced Deanonymization through Strava," *Steve Loughran* (blog), January 29, 2018, http://steveloughran.blogspot.com/2018/01/advanced-denanonymization-through-strava.html.
[10] Until recently, avoiding each of those vulnerabilities required a unique opt-out beyond the strictest general privacy setting. Despite recent privacy updates and regardless of the privacy setting selected, the information *Strava* sells from all its users can still create a similar level of exposure. See Rosie Spinks, "Using a Fitness App Taught Me the Scary Truth about Why Privacy Settings Are a Feminist Issue," *Quartz* (blog), August 1, 2017, https://qz.com/1042852/using-a-fitness-app-taught-me-the-scary-truth-about-why-privacy-settings-are-a-feminist-issue/; Ashley Carman, "Strava Will Refresh Its Heat Map Every Month to Clear It of Data That Recently Went Private," The Verge, March 13, 2018, https://www.theverge.com/2018/3/13/17115810/strava-heat-map-update-refresh-private.
[11] Alex Hern, "Strava Suggests Military Users 'opt out' of Heatmap as Row Deepens," The Guardian, January 29, 2018, http://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban.
[12] Ibid.
[13] John Goolgasian is the former-Director of the Foundation GEOINT Group, Source and Operations Management Directorate, NGA. See "Value in GEOINT," The National Geospatial Intelligence Journal, accessed March 15, 2018, http://sites.psu.edu/thenationalgeospatialintelligencejournal/value-in-geoint/.
[14] Scott A. Bryant, "Geospatial Informational Security Risks and Concerns of the United States Air Force Geobase Program" (Air Force Institute of Technology, 2007), http://www.dtic.mil/dtic/tr/fulltext/u2/a465293.pdf.
[15] John C. Baker et al., *Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information* (RAND National Defense Research Institute, 2004), 122, https://www.rand.org/pubs/monographs/MG142.html.
[16] George Bush, "Statement on Signing the Land Remote Sensing Policy Act of 1992," The American Presidency Project, October 28, 1992, http://www.presidency.ucsb.edu/ws/?pid=21693.
[17] Users of civilian GPS were instantly able to determine locations up to ten times more accurately. See Bill Clinton, "Statement by the President Regarding the United States' Decision to Stop Degrading Global Positioning System Accuracy," May 1, 2000, https://clintonwhitehouse3.archives.gov/WH/EOP/OSTP/html/0053_2.html.
By 2007, the United States stopped procuring GPS satellites that had Selective Availability capabilities. See Dana Perino, "Statement by the Press Secretary," September 18, 2007, https://georgewbush-whitehouse.archives.gov/news/releases/2007/09/20070918-2.html.

[18] "Civilian Benefits of Discontinuing Selective Availability," GPS.gov, May 1, 2000, https://www.gps.gov/systems/gps/modernization/sa/benefits/. The economic benefits proved to be significant—Simon Greenman, co-founder of MapQuest.com, cites turning off Selective Availability as "when many of us from the [geographic information systems (GIS)] industry saw the power of the Internet to bring mapping to the masses for free." See Jerry Brotton, *A History of the World in Twelve Maps* (New York: Viking, 2012), 420.
[19] Brotton, *A History of the World in Twelve Maps*, 420.
[20] Just four years after its 2009 founding, Foursquare's users had checked in over one billion times. Those check-ins provide the company with a significant database of user activity from which to generate user-specific content. Robert Scoble and Shel Israel, *Age of Context* (Patrick Brewster Press, 2014), 19.
[21] For tracking crowd sizes, see "BLINK Cincinnati - Apps on Google Play," accessed October 13, 2017, https://play.google.com/store/apps/details?id=com.blinkcincinnati.blink. For tracking buses, see "Better Real-Time Transit Data Is Coming to Your City (Finally)," Medium, December 20, 2016, https://medium.com/transit-app/better-real-time-transit-data-is-coming-to-your-city-finally-a38ed0e90084.
[22] Geofencing establishes a virtual perimeter around a given point. Tracking users' devices' locations allows companies to detect when they enter the geofenced area and send a timely, location-based notification. See Chirag Kulkarni, "15 Ways Geolocation Is Totally Changing Marketing," Fortune, February 6, 2017, http://fortune.com/2017/02/06/geolocation-marketing/.
[23] Ishveena Singh, "The Perfect Storm Called Artificial Intelligence and Geospatial Big Data," *Geoawesomeness* (blog), November 14, 2017, http://geoawesomeness.com/the-perfect-storm-called-artificial-intelligence-and-geospatial-big-data/.
[24] Adam Van Etten, "Car Localization and Counting with Overhead Imagery, an Interactive Exploration," *Medium* (blog), March 15, 2017, https://medium.com/the-downlinq/car-localization-and-counting-with-overhead-imagery-an-interactive-exploration-9d5a029a596b.
[25] Public GEOINT had an immediate impact. Just three months after its release, Google Earth facilitated rescue missions and recovery work in the wake of Hurricane Katrina. Since then public GEOINT has assumed a greater role in crisis response efforts. See Andrew Foerch, "The Genesis of Google Earth," *Trajectory Magazine* (blog), November 1, 2017, http://trajectorymagazine.com/genesis-google-earth/.
[26] "Burma: New Satellite Images Confirm Mass Destruction," Human Rights Watch, October 17, 2017, https://www.hrw.org/news/2017/10/17/burma-new-satellite-images-confirm-mass-destruction.
[27] Anna Fifield, "New Images Show North Korea's Extensive Network of 'Reeducation' Camps," *Washington Post*, October 26, 2017, sec. Asia & Pacific, https://www.washingtonpost.com/world/asia_pacific/new-images-show-north-koreas-extensive-network-of-re-education-camps/2017/10/25/894afc1c-b9a7-11e7-9b93-b97043e57a22_story.html.
[28] "Burundi: Satellite Evidence Supports Witness Accounts of Mass Graves," January 28, 1920, https://www.amnesty.org/en/latest/news/2016/01/burundi-satellite-evidence-supports-witness-accounts-of-mass-graves/.
[29] Steven Livingston, "Satellite Imagery Augments Power and Responsibility of Human Rights Groups," *Brookings* (blog), June 23, 2016, https://www.brookings.edu/blog/techtank/2016/06/23/satellite-imagery-augments-power-and-responsibility-of-human-rights-groups/.
[30] Scrutinizing the vast data flows requires the efforts of thousands of volunteers on short notice. As a result, most crisis mapping groups are disparate communities of mappers who activate when disaster strikes. The power of their work was seen in the aftermath of the April 2015 Nepal earthquake. Immediately after the quake, the Standby Task Force crowdsourced the analysis of tweets and mainstream media reports to assess damage and identify where humanitarian groups were deploying. The Humanitarian UAV Network produced extensive imagery, which Humanitarian OpenStreetMap and MicroMappers then pushed to their volunteer networks for analysis and projection on their live, publicly-available crisis maps. See S Kulshrestha, "Cutting-Edge Engineering For Modern Geospatial Systems," *Geointelligence* 5, no. 3 (June 2015): 18.
[31] Hannah Bloch, "When Disaster Strikes, He Creates A 'Crisis Map' That Helps Save Lives," NPR, October 2, 2016, https://www.npr.org/sections/parallels/2016/10/02/495795717/when-disaster-strikes-he-creates-a-crisis-map-that-helps-save-lives.
[32] In August 2015, the NGA launched the GEOINT Pathfinder project to help the agency take advantage of improving public GEOINT capabilities. The project uses exclusively unclassified tools, data, and services from the commercial and open source communities. Chris Rasmussen, who heads the GEOINT Pathfinder project, says the NGA is adopting commercial GEOINT because "that's where the data's at." See "GEOINT Pathfinder Project Yields New Open Source Coding Projects Available to Public," National Geospatial-Intelligence Agency, February 22, 2016, https://www.nga.mil/MediaRoom/PressReleases/Pages/GEOINT-Pathfinder-project-yields-new-open-

source-coding-projects-available-to-public.aspx; Phillip Swarts, "How the NGA Is Learning to Stop Worrying and Love Open-Source Data," *Space News Magazine* (blog), December 19, 2016, http://www.spacenewsmag.com/feature/how-the-nga-is-learning-to-stop-worrying-and-love-open-source-data/; Frank Konkel, "Why Open Data Is the Future of the National Geospatial-Intelligence Agency," Nextgov.com, June 29, 2015, http://www.nextgov.com/emerging-tech/emerging-tech-blog/2015/06/why-open-data-future-national-geospatial-intelligence-agency/116551/.

[33] The NGA also posts projects on GitHub. See Adam Stone, "Open-Source Intel: NGA Taps Crowd for Better Tools," C4ISRNET, April 26, 2016, http://www.c4isrnet.com/intel-geoint/2016/04/26/open-source-intel-nga-taps-for-better-tools/.

[34] Daniel Cebul, "Finding a Tent in a Satellite Image Is the New Needle in a Haystack," C4ISRNET, March 7, 2018, http://www.c4isrnet.com/intel-geoint/2018/02/26/finding-a-tent-in-a-satellite-image-is-the-new-needle-in-a-haystack/.

[35] "Commercial GEOINT Strategy" (National Geospatial-Intelligence Agency, October 2015), https://www.nga.mil/MediaRoom/PressReleases/Documents/2015/NGA_Commercial_GEOINT_Strategy.pdf.

[36] In a December 2016 interview, Chris Rasmussen observed that "From our perspective, the more [commercial satellite] subscriptions that are available, the more analytics services that are available to consume from these [public GEOINT] organizations, the better." Swarts, "How the NGA Is Learning to Stop Worrying and Love Open-Source Data."

[37] The rise of the global location of things market—which is expected to grow at a compound annual growth rate of 34.07 percent, reaching 76.1 billion dollars by 2025—is producing an ever-growing stream of geospatial information. See "Location of Things Market Analysis, by Application (Mapping & Navigation, Asset Management, Location Intelligence, Media Engagement), by Vertical, by Region and Segment Forecasts, 2014 - 2025," Grand View Research, August 2017, https://www.researchandmarkets.com/reports/4396482/location-of-things-market-analysis-by. For aerial imagery market trends, see "Aerial Imagery Market Size, Share, Industry Report, 2023," November 2017, https://www.psmarketresearch.com/market-analysis/aerial-imagery-market.

[38] Andrew McAfee and Erik Brynjolfsson, *Machine, Platform, Crowd* (W.W. Norton & Company, 2017), 308.

[39] McAfee and Brynjolfsson, 235.

[40] The International Data Corporation predicts wearable device shipments to nearly double by 2021 to 222.3 million devices shipping annually. See "IDC Forecasts Shipments of Wearable Devices to Nearly Double by 2021 as Smart Watches and New Product Categories Gain Traction," International Data Corporation, December 20, 2017, https://www.idc.com/getdoc.jsp?containerId=prUS43408517.

[41] Goodman, *Future Crimes*, 189–90.

[42] With networks of officers, closed-circuit cameras, and helicopters, the police have historically had superior tactical information during public events like protests. However, crowdsourcing applications like *Sukey* can give the public more observation points than the police. If protestors have greater volumes of more granular intelligence than law enforcement agencies, they can significantly change protest dynamics by making more informed tactical maneuvers. See Tim Dees, "Rioters Using Google Maps for Real-Time Information," PoliceOne, December 28, 2010, https://www.policeone.com/police-products/police-technology/articles/3115790-Rioters-using-Google-Maps-for-real-time-information/; Patrick Kingsley, "Inside the Anti-Kettling HQ," The Guardian, February 3, 2011, http://www.theguardian.com/uk/2011/feb/02/inside-anti-kettling-hq; Goodman, *Future Crimes*, 190.

[43] Former Central Intelligence Agency director David Petraeus noted that the internet of things will be "transformational for clandestine tradecraft." See Spencer Ackerman, "CIA Chief: We'll Spy on You Through Your Dishwasher," Wired, March 15, 2012, https://www.wired.com/2012/03/petraeus-tv-remote/.

[44] "Mobile Phone Users Worldwide 2013-2019," Statista, 2018, https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/.

[45] Alex Hern, "Three Quarters of Android Apps Track Users with Third Party Tools – Study," The Guardian, November 28, 2017, http://www.theguardian.com/technology/2017/nov/28/android-apps-third-party-tracker-google-privacy-security-yale-university.

[46] Early augmented reality apps include the game *Pokémon Go* and L'Oreal's virtual art exhibit application which tracked users to produce a heatmap logo. See Tarun Wadhwa, "CrowdOptic and L'Oreal To Make History By Demonstrating How Augmented Reality Can Be A Shared Experience," Forbes, June 3, 2013, https://www.forbes.com/sites/tarunwadhwa/2013/06/03/crowdoptic-and-loreal-are-about-to-make-history-by-demonstrating-how-augmented-reality-can-be-a-shared-experience/.

[47] Stipica Šarčević, "Map of Business Structure and Activity in Zagreb," *GIS Cloud* (blog), January 25, 2018, https://www.giscloud.com/blog/map-of-business-structure-and-activity-in-city-districts-of-zagreb/.

[48] Alex Woodie, "5 Ways Big Geospatial Data Is Driving Analytics In the Real World," Datanami, May 21, 2015, https://www.datanami.com/2015/05/21/5-ways-big-geospatial-data-is-driving-analytics-in-the-real-world/.
[49] Patrick C. Miller, "The Latest News on Unmanned Aerial Systems - Consumer Drone Sales Expected to Skyrocket in Coming Decade," UAS Magazine, January 21, 2016, http://www.uasmagazine.com/articles/1403/consumer-drone-sales-expected-to-skyrocket-in-coming-decade.
[50] Matt Alderton, "The Insight Economy," *Trajectory Magazine* (blog), August 16, 2017, http://trajectorymagazine.com/the-insight-economy/.
[51] Strava Metro sells users' data at a rate of about $0.80 per user per year. The data provides cities unparalleled insight into the flow of their traffic. See Mike Wehner, "Strava Begins Selling Your Data Points, and No, You Can't Opt-Out," Engadget, May 23, 2014, https://www.engadget.com/2014/05/23/strava-begins-selling-your-data-points-in-the-hopes-of-creating/; Kelsey Campbell-Dollaghan, "How Strava, The App For Athletes, Became An App For Cities," Co.Design, November 1, 2017, https://www.fastcodesign.com/90149130/strava-the-app-for-athletes-is-becoming-an-app-for-cities; Alex Davies, "Strava's Cycling App Is Helping Cities Build Better Bike Lanes," Wired, June 3, 2014, https://www.wired.com/2014/06/strava-sells-cycling-data/.
[52] There are three main ways to deanonymize location data. 1) In some cases, as with *Strava* segment spoofing, the company providing the data will deanonymize certain data itself. See Matt Burgess, "Strava's Data Lets Anyone See the Names (and Heart Rates) of People Exercising on Military Bases," Wired UK, accessed March 9, 2018, http://www.wired.co.uk/article/strava-military-bases-area-51-map-afghanistan-gchq-military. 2) Recent studies have found that the uniqueness of human traces makes them relatively easy to disaggregate without much other data. In fact, just four spatio-temporal points is usually enough to identify a user. See Hui Zang and Jean Bolot, "Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study," *MobiCom '11 Proceedings of the 17th Annual International Conference on Mobile Computing and Networking*, n.d., 145–56, https://doi.org/10.1145/2030613.2030630; Yves-Alexandre de Montjoye et al., "Unique in the Crowd: The Privacy Bounds of Human Mobility," *Scientific Reports* 3, no. 1376 (March 25, 2013), https://doi.org/10.1038/srep01376; Chris Riederer et al., "Linking Users Across Domains with Location Data: Theory and Validation," *International World Wide Web Conference*, April 11, 2016, https://doi.org/10.1145/2872427.2883002. 3) When location-tracking information is combined with other personal data for sale or otherwise available, it can be readily reidentified revealing a detailed user profile. See D. J. Pangburn, "Even This Data Guru Is Creeped Out By What Anonymous Location Data Reveals About Us," Fast Company, September 26, 2017, https://www.fastcompany.com/3068846/how-your-location-data-identifies-you-gilad-lotan-privacy.
[53] Vricon offers three-dimensional mapping services, see "3D Surface Model," *Vricon* (blog), accessed March 5, 2018, https://www.vricon.com/products/vricon-data-suite/3d-surface-model-video/. TerraGo provides offline mapping services, see "Agriculture," accessed March 30, 2018, https://www.terragotech.com/solutions/by-industry/agriculture.
[54] "Descartes Labs: Home," Descartes Labs, accessed February 24, 2018, https://www.descarteslabs.com/.
[55] Sarah Scoles, "The Race to Rule the High-Flying Business of Satellite Imagery," Wired, March 28, 2017, https://www.wired.com/2017/03/race-rule-high-flying-business-satellite-imagery/.
[56] Goodman, *Future Crimes*, 81.
[57] Initial fears about the dangers of Google Earth and social media geotagging have not been fully realized, because they conflated volume of information available with volume of actionable insights. While the volume of information available continues to grow exponentially, the growing volume of actionable intelligence now mirrors that trend. That is what makes real-time remote reconnaissance so dangerous. See Goodman, 28.
[58] Goodman, 2.
[59] Gerald Friedland and Robin Sommer, "Cybercasing the Joint: On the Privacy Implications of Geo-Tagging" (Berkeley, California: International Computer Science Institute, May 3, 2010), http://www.icsi.berkeley.edu/pubs/techreports/TR-10-005.pdf.
[60] Geotagging has also revealed that soldiers were operating where their government said they were not. In July 2014, Russian communications specialist Alexander Sotkin uploaded pictures of himself—including a picture with him posing in a military uniform—in Krasna Talychka, a rebel-controlled village in east Ukraine. See Joe Murphy, "Soldier's Web Selfies Reveal Illicit Russian Operations in Ukraine," Evening Standard, July 31, 2014, http://www.standard.co.uk/news/world/soldier-s-web-selfies-reveal-illicit-russian-operations-in-ukraine-9639708.html. Similarly, in November 2015, geotagged pictures uploaded to social media show men known to have served in the Russian armed forced posing with military equipment in Syria. These images repudiated Russia's claim that it had no troops on the ground in Syria. In October 2017, Russia proposed banning military personnel from taking selfies to prevent self-published images from revealing—often within several meters—where units had been deployed. See Maria Tsvetkova, "Russian Soldiers Geolocated by Photos in Multiple Syria Locations,

Bloggers Say," *Reuters*, November 8, 2015, https://www.reuters.com/article/us-mideast-crisis-syria-russia/russian-soldiers-geolocated-by-photos-in-multiple-syria-locations-bloggers-say-idUSKCN0SX0H820151108; "Russian Soldiers Face Ban on Selfies," *BBC News*, October 5, 2017, sec. Europe, http://www.bbc.com/news/world-europe-41510592.

[61] Cheryl Rodewig, "Geotagging Poses Security Risks," www.army.mil, March 7, 2012, https://www.army.mil/article/75165/geotagging_poses_security_risks.

[62] Goodman, *Future Crimes*, 115.

[63] Alyona Zhuk, "War In The Age Of Social Media," Kyiv Post, July 4, 2015, https://www.kyivpost.com/article/content/war-against-ukraine/war-in-the-age-of-social-media-392572.html.

[64] Thomas Harding, "Terrorists 'Use Google Maps to Hit UK Troops,'" *The Telegraph*, January 13, 2007, sec. World, https://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html.

[65] Goodman, *Future Crimes*, 28–29.

[66] "How Terrorists Carried out Pathankot Attack: Google Maps to Plan, Facebook to Connect," *The Financial Express*, December 20, 2016, http://www.financialexpress.com/india-news/how-terrorists-carried-out-pathankot-attack-google-maps-to-plan-facebook-to-connect/480294/.

[67] "Pathankot Attack: Sensitive Sites on Google Maps under Delhi HC Scanner," Gadgets Now, 2016, https://www.gadgetsnow.com/tech-news/Pathankot-attack-Sensitive-sites-on-Google-Maps-under-Delhi-HC-scanner/articleshow/50596143.cms.

[68] "How Terrorists Carried out Pathankot Attack."

[69] "Mumbai Terrorists' Use of Google Earth Re-Ignites Concerns," Homeland Security Today, December 5, 2008, https://www.hstoday.us/kimery-report/mumbai-terrorists-use-of-google-earth-re-ignites-concerns/.

[70] James Glanz, Sebastian Rotella, and David E. Sanger, "In 2008 Mumbai Attacks, Piles of Spy Data, but an Uncompleted Puzzle," *The New York Times*, December 21, 2014, sec. Asia Pacific, https://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html.

[71] If this granular, local-level information is converted to a virtual reality format, attackers could literally walk-through the attack in training. Public virtual reality training simulations are already being developed, see Sidney Fussell, "Bleak New Game Trains Teachers How to Survive School Shootings," Gizmodo, accessed April 1, 2018, https://gizmodo.com/new-vr-simulation-trains-teachers-how-to-act-during-sch-1821736475.

[72] "Emerging Opportunities and Reasons to Invest in GIS Technology.," Business Mapper, accessed February 4, 2018, http://businessmapper.biz/articles/emerging-opportunities-and-reasons-to-invest-in-gis-technology.

[73] Jeremy Kahn, "Mumbai Terrorists Relied on New Technology for Attacks," *The New York Times*, December 8, 2008, sec. Asia Pacific, https://www.nytimes.com/2008/12/09/world/asia/09mumbai.html.

[74] Goodman, *Future Crimes*, 235.

[75] Robert Cardillo, The concept of counter-GEOINT, interview by Francis Rose, January 22, 2017, https://govmatters.tv/the-concept-of-counter-geoint/.

[76] If a country's government asks, all satellite imagery companies are expected to disclose what portion of their territory was photographed and offer to sell the imagery to them at the market rate. See Laurence Nardon, "Satellite Imagery Control: An American Dilemma" (Paris: The Centre français sur les Etats-Unis, March 2002), https://www.ifri.org/sites/default/files/atoms/files/imageriesatellitaireln0302.pdf.

[77] For a discussion of U.S. Remote Sensing Regulations, see Robert A. Weber and Kevin M. O'Connell, "Alternative Futures: United States Commercial Satellite Imagery in 2020" (Innovative Analytics & Training, November 2011), sec. Appendix A, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB404/docs/37.pdf.

[78] For example, the Kyl-Bingaman Amendment prohibits U.S. companies from releasing high-resolution images of Israel and the occupied territories. Israel has asked other countries to impose similar restrictions, but not all do. See Hamed Aleaziz, "Why Google Earth Can't Show You Israel," *Mother Jones* (blog), June 10, 2011, https://www.motherjones.com/politics/2011/06/google-israel-us/.

[79] Although companies are prohibited from selling imagery to certain countries and terrorist organizations on the State Department's prohibited purchaser list, potential adversaries can circumvent those rules by creating a fictitious organization or employing a third-party purchaser. See Raphael Prober, "Shutter Control: Confronting Tomorrow's Technology with Yesterday's Regulations," *Journal of Law & Politics* 19, no. 2 (Spring 2003): 203–51.

[80] Michelle L. Aten and Mark A. Hover, "Assessment of the U.S. Policy of Shutter Control and Its Impact on U.S. Commercial Remote Sensing Firms," in *Sensors, Systems, and Next-Generation Satellites IV*, vol. 4169 (Sensors, Systems, and Next-Generation Satellites IV, International Society for Optics and Photonics, 2001), 392–96, https://doi.org/10.1117/12.417144.

[81] Also known as "buy to deny." See Pat Norris, *Watching Earth from Space: How Surveillance Helps Us -- and Harms Us* (Springer Science & Business Media, 2010), 200.
[82] The United States, and select other customers, can also hire commercial satellite imagery companies to take certain images without making them available to other users. See Sarah Scoles, "How the Government Controls Sensitive Satellite Data," Wired, February 8, 2018, https://www.wired.com/story/how-the-government-controls-sensitive-satellite-data.
[83] Sharon Weinberger, "ISpy: National Security in the Era of Google Earth," Wired, July 22, 2008, https://www.wired.com/2008/07/ispy-national-s/. Later in the conflict, an Israeli firm circumvented the U.S. blackout and sold high-resolution imagery. See Ram S. Jakhu, *National Regulation of Space Activities* (Springer, 2010), 455, https://books.google.com/books?id=2oQ7dcXvt0YC&pg=PA455&lpg=PA455&dq=u.s.+shutter+control+policy&source=bl&ots=FsubHPNshZ&sig=0sH2Y6GNrdOvgVEDWepcmmAz0II&hl=en&sa=X&ved=0ahUKEwjsmdTF-oPaAhWRtlMKHS-hBSwQ6AEIVTAI#v=onepage&q=u.s.%20shutter%20control%20policy&f=false.
[84] The proliferation of high-resolution satellite systems, especially those that are not licensed in the United States, decreases the likelihood that the U.S. government can buy exclusive rights to all the imagery of a given area for an extended period of time. James A. Vedda, "U.S. National Security and Economic Interests in Remote Sensing: The Evolution of Civil and Commercial Policy" (National Geospatial-Intelligence Agency, February 20, 2009), https://fas.org/irp/eprint/remote.pdf.
[85] Overseas companies and foreign states can sell satellite imagery that American companies cannot. For example, in 1990 the St. Petersburg Times bought and analyzed Soviet imagery, revealing that Iraq had far fewer troops in Kuwait than the U.S. government had claimed. See Jean Heller, "U.S. Satellites Won't Be Watching Alone," St. Petersburg Times, March 15, 2003, https://www.globalsecurity.org/org/news/2003/030315-satellites01.htm.
[86] For example, Google Street Map revealed the road layout on several U.S. military bases in 2007. The information, which Colonel James Brown called "the best preoperational surveillance tool I've ever seen in my life," was removed, only to have *Strava* reveal the same type of routes years later. See Sharon Weinberger, "Can You Spot the Chinese Nuclear Sub?," Discover Magazine, July 21, 2008, http://discovermagazine.com/2008/aug/21-can-you-spot-the-chinese-nuclear-sub.
[87] The limitations of domestic censorship were revealed in the early days of commercial satellite imagery. U.S.-based Aerial Images released Russian photos of Area 51 when other American companies declined to provide the imagery. See William J. Broad, "Ideas & Trends; Snooping's Not Just For Spies Any More," *The New York Times*, April 23, 2000, sec. Week In Review, https://www.nytimes.com/2000/04/23/weekinreview/ideas-trends-snooping-s-not-just-for-spies-any-more.html.
[88] It is illegal in the United States—even for law enforcement agencies—to use devices that jam Global Positioning System (GPS) signals, because they are so effective at disrupting GPS devices in the area. By sending noise on the same frequencies as satellites, the jammers prevent GPS receivers from picking up the correct signals. This successfully renders GPS tracking impossible. See Kashmir Hill, "Jamming GPS Signals Is Illegal, Dangerous, Cheap, and Easy," Gizmodo, July 24, 2017, https://gizmodo.com/jamming-gps-signals-is-illegal-dangerous-cheap-and-e-1796778955.
[89] Walter Scott, "U.S. Satellite Imaging Regulations Must Be Modernized," SpaceNews.com, August 29, 2016, http://spacenews.com/op-ed-u-s-satellite-imaging-regulations-must-be-modernized/.
[90] Scoble and Israel, *Age of Context*, 15.
[91] "GIS: The Backbone of Homeland Security," Homeland Security Today, September 26, 2012, https://www.hstoday.us/daily-briefings-newsletter-cybersecurity-and-it-wnb-cybersecurity-today/gis-the-backbone-of-homeland-security/.

The Project on International Peace and Security (PIPS)
Institute for the Theory and Practice of International Relations
The College of William and Mary