NTI
BUILDING A SAFER WORLD

Innovating Verification: New Tools & New Actors to Reduce Nuclear Risks

Redefining Societal Verification

PART OF THE *Cultivating Confidence Verification Series*

About the Verification Pilot Project

The Verification Pilot Project of the Nuclear Threat Initiative (NTI) convened technical and policy experts from around the world to develop recommendations for new approaches to verification that could enable future progress on arms reductions. As the two-year project moved forward, it became clear that innovating verification could also prompt near-term progress on non-proliferation and nuclear security.

NTI partnered with senior leaders from the U.S. Departments of Defense, Energy, and State as well as the governments of Norway, Sweden, and the United Kingdom. That dialogue identified the key challenges that became the subjects of the project's three expert working groups, which included more than 40 technical and policy experts from a dozen countries. *Innovating Verification: New Tools & New Actors to Reduce Nuclear Risks* includes an overview and reports from the three working groups:

- The ***Innovating Verification Overview*** includes a foreword by Sam Nunn, NTI's chief executive officer and co-chairman, and key project findings and recommendations across report topics.
- ***Verifying Baseline Declarations of Nuclear Warheads and Materials*** analyzes how baseline declarations can contribute to near- and long-term arms control and non-proliferation goals and how to verify them without compromising sensitive information.
- ***Redefining Societal Verification*** explores how advances in information technologies, big data, social media analytics, and commercial satellite imagery can supplement existing verification efforts by governments and increase contributions from outside experts.
- ***Building Global Capacity*** considers the value of expanded international participation in the verification of nuclear arms reductions and how this participation can increase confidence in nuclear threat reduction efforts among all states.

The project builds on *Cultivating Confidence: Verification, Monitoring, and Enforcement for a World Free of Nuclear Weapons* (Nuclear Threat Initiative, 2010), which outlined key issues that states need to address to ensure that nuclear weapons reductions can proceed in a safe and transparent manner.

NTI
BUILDING A SAFER WORLD

Innovating Verification: New Tools & New Actors to Reduce Nuclear Risks

Redefining Societal Verification

July 2014

PART OF THE *Cultivating Confidence Verification Series*

Cover Images: © iStockphoto

Print Report Design: Dinsmore Designs

The views expressed in this publication do not reflect those of the NTI Board of Directors or institutions with which they are associated.

Contents

Acknowledgments

This report would not have been possible without the contributions of many.

We are extremely grateful for the advice and input of the senior government officials who helped shape this effort from the beginning. In the United States, this list includes Donald L. Cook, Rose E. Gottemoeller, Anne Harrington, and Andrew C. Weber; in the United Kingdom, Bryan Wells and Peter Sankey from the Ministry of Defence; Norwegian Ambassador Kåre Aas; and Christer Ahlstrom at the Swedish Ministry for Foreign Affairs. We also thank Richard Gullikson and Gary Stradling of the United States Defense Threat Reduction Agency and Kjetil Køber of the Norwegian Ministry of Foreign Affairs.

We are grateful to NTI Co-Chairman and Chief Executive Officer Sam Nunn, Vice Chairman Des Browne, President Joan Rohlfing, and Executive Vice President Deborah Rosenblum for their strategic vision and collective feedback. We would also like to thank the NTI Board of Directors for their ongoing support, in particular NTI President Emeritus Charles B. Curtis.

Achieving the central aims of this project would not have been possible without our working group members. These highly respected experts have been extremely generous with their time and energy, and we have done our best to ensure that this project reflects their collective wisdom.

We also appreciate the many officials and experts who briefed the working group and provided critical insights. Special thanks to Douglas J. Naquin, Dylan Schmorrow, Lisa Costa, Jill Egeth and their team at MITRE; Anthony Stefanidis, Arie Croitoru, Andrew Crooks and Jacek Radzikowski from the George Mason Center for Geospatial Intelligence; and Paul Richards from Columbia University.

Finally, we are indebted to all our colleagues at NTI. In particular, we thank Carmen MacDougall and Mimi Hall for their guidance and communications expertise. Special thanks are due to Elise Rowan who managed the production of the project's results to a successful conclusion. Tammy Ware was indispensible to the success of the project as her support was both professional and personal to us and to all the working group members. We also are grateful to interns Lauren Callahan and Sahil Shah and to Herbert Scoville Jr. Peace Fellow Jessica Bufford for their contributions to the project.

Corey Hinderstein
Vice President, International Program

Andrew Newman, Ph.D.
Senior Program Officer, International Program

Kelsey Hartigan
Program Officer, International Program

Contributors

REDEFINING SOCIETAL VERIFICATION WORKING GROUP

Chair: Corey Hinderstein
Vice President, International Program
Nuclear Threat Initiative

Erica Briscoe, Ph.D.
Senior Research Scientist
Georgia Tech Research Institute

Kelsey Hartigan
Program Officer, International Program
Nuclear Threat Initiative

Richard W. (Chip) Hartman II
Executive Director, International Security Advisory Board
U.S. Department of State

Bryan Lee
Director of the Eurasia Nonproliferation Program
James Martin Center for Nonproliferation Studies
Monterey Institute of International Studies

Timothy Miller
Contractor, Toeroek Associates
U.S. Department of Defense

Frank Pabian, Ph.D.
Fellow, Los Alamos National Laboratory
Senior Open-Source Nonproliferation Analyst, Joint Research Centre
European Commission

Kurt K. Siemon, Jr.
Director of the Office of Nuclear Verification, Office of Nonproliferation and International Security
National Nuclear Security Administration
U.S. Department of Energy

Kevin Whattam, Ph.D.
Manager, Nonproliferation and International Security
Pacific Northwest National Laboratory

Daniel Wurmser, Ph.D.
Physical Science Officer, Bureau of Arms Control, Verification, and Compliance
U.S. Department of State

Tong Zhao
Stanton Nuclear Security Predoctoral Fellow, Managing the Atom Project/International Security Program
Harvard University
Ph.D. Candidate
Georgia Institute of Technology

Members of the Nuclear Threat Initiative's Verification Pilot Project endorse the general tenor of this report but were not asked to support each individual finding and recommendation. The views expressed in this report do not reflect those of the institutions with which the working group members are associated. Their affiliations are listed for the purpose of identification only.

1. Executive Summary

Applying Transformative Technologies to Arms Control and Non-Proliferation Verification

> *A new facility appears in a country that has made specific treaty-based commitments regarding its nuclear weapons program. A blogger popular with nuclear experts posts a commercial satellite image and asks the community: What is this? Satellite imagery analysts, regional specialists, technical experts, native language speakers, and specialists from other disciplines, some not related to nuclear weapons or their associated technologies, weigh in. They assemble a compelling circumstantial case that the activity at the facility is suspicious.*
>
> *In parallel, officials from the treaty partners assess what is happening and decide whether the facility is unrelated to treaty obligations or houses secret, proscribed activities. In addition to the information the outside experts have generated, government officials tap classified resources, including spy satellites, and purchase commercial satellite imagery of areas where national satellites did not focus or have a clear view. Open-source intelligence analysts, meanwhile, scour local native-language media for clues and check chatter. They also comb social media for references that could indicate the purpose of the building, and they search photo and video-sharing sites for images that show activity at the facility. Companies specializing in crucial, difficult-to-acquire materials are consulted to see if there have been attempted (or successful) procurements. Analysts combine all of the information, including from formal verification tools, to determine whether the country is using the facility to violate its treaty commitments.*

The fictional scenario above raises important questions. Are governments prepared to use all the information-gathering and analysis tools at their disposal to respond to possible treaty violations? Do states understand the privacy and personal data protection issues related to these new areas of data collection? Are states prepared to respond if their private conclusion is different from the one reached by outside experts, whose analysis is public? The answer today to all those questions is no.

Information and communication technologies (ICT) have reshaped how countries, corporations, and private citizens share, collect, and analyze information. As global communication technologies have increased, so too has the amount of publicly generated data. The big data phenomenon has led to groundbreaking innovations in emergency response, humanitarian relief, disease control, and commercial marketing and sparked interest in the nuclear arms control and non-proliferation domains.

Opportunities for strengthening a 21st-century verification regime could abound if public and private resources are focused on benefiting from societal verification tools, but significant issues must be understood.

This report redefines societal verification as a process by which states or international organizations can use information generated and communicated by individuals or expert communities for arms control or non-proliferation treaty verification. It should be based on sound, tested, and validated procedures that take advantage of the data now available to states. It would not rely on luck in finding a specific piece of information, mysterious analytical processes, or the tasking of citizens to become whistleblowers or amateur spies. The system of data collection and analysis developed for arms control or non-proliferation treaty verification can also contribute to broader nuclear confidence building and threat reduction.

The concept of societal verification, in some form or another, is not new, but ideas about how societal verification might contribute to state efforts have evolved in recent years. Even though state systems have not yet caught up to the promise of societal verification, in a world of abundant data and perpetual connectivity, the technical has joined the conceptual, making some level of societal verification a real possibility in a way that was not previously achievable.

With the vast amount of information available today, external analysis will continue to improve, whether or not governments leverage new media themselves or embrace the potential contribution of outside experts to treaty verification efforts. Accessible technical capacity, like smartphones with wireless communications connectivity, built-in sensors and geolocation capabilities, and data storage and processing capability continues to improve and expand. These capabilities offer knowledgeable citizens powerful tools to collect and share information.

Arms control verification has relied almost exclusively on tools such as on-site inspections and satellite imagery. Through societal verification, states can leverage new technologies and publicly available data to supplement national technical means (NTM) and other traditional verification methods.

Some emerging transformative technologies provide new information (geospatial data), and some are new means to transmit or widen the exposure of existing information (social media). To use these tools, states must decide which steps are most suitable for near-term application and which require further bureaucratic, institutional, diplomatic, and technical development.

A system's ability to adapt to and incorporate emerging technologies is often slower than the emergence of the technologies themselves. As the introduction of the telegraph and radio proved, it is difficult to predict the value of technology and new data as it is emerging, and the private sector and general public often prove more innovative and creative than governments in using the new tools.

The biggest challenges to data utilization are systemic and organizational rather than technical. Verification of treaties and compliance with agreements are fundamentally policy judgments made by states. This reality needs to drive any discussion of who collects what and how, to make a conclusion about whether states are meeting treaty obligations.

There are two primary points of input for societal verification data: analysis within government verification systems and analysis by outside expert communities. Regarding the process of data collection and analysis inside governments, there may be value to treating societal verification data like other open-source information for the purpose of cooperative monitoring and integration into state-level conclusions about treaty compliance. If states explicitly add these sources to their pool of knowledge, they can also include information generated by outside analytical communities. This second track is an independent path to identify and assess new sources of data and can contribute to official deliberations. Both tracks can utilize a diverse set of tools and function on a continuum from observing, or simply gathering information already being generated for other purposes, to mobilizing—that is, engaging with individuals or groups to generate new data.

The joining of data, communication methods, and technology transforms how the world looks at information, analysis, and dissemination. For arms control verification, a well-developed and integrated program to access societal verification data would prove at least additive to current treaty verification efforts and may dwarf the contribution of current open-source data. Societal verification could transform treaty verification, particularly in addressing the specific challenges posed by identifying undeclared and prohibited facilities or activities. Opportunities for strengthening a 21st-century verification regime could abound if public and private resources are focused on benefiting from societal verification tools, but significant issues must be understood before it becomes possible to calculate the value of such tools.

There is a pressing need to build and identify expert communities to participate in societal verification efforts. Communities of practice are reservoirs of knowledge. Some of these groups are part of traditional arms control stakeholder communities and some are not, and it is not always obvious who belongs or should belong. Having a reliable cadre of experts who are interested and prepared to assist in verification would be valuable to states and international organizations. Ad hoc and temporary analytic groups with diverse expertise can be formed akin to flash mobs. They are task oriented, and effective in meeting short-term, analytic challenges. With the consistent voices of permanent or temporary groups evaluating publicly available data, states will more easily and openly be held accountable for their public conclusions about treaty implementation and compliance.

Current technology and analytical tools have not yet shown that they can predict behavior, but verification is not forward looking; it is backward looking, focused upon an activity or event that has already occurred. Even with this somewhat simpler task, gaining a situational understanding requires a multidisciplinary approach, from computer science to sociology. Investing in societal verification with sustained engagement from the technical and policy communities can foster this approach.

Issues of privacy, data confidentiality, and legal oversight must be managed. Societal norms influence whether and how societal verification can be used in different countries. These issues are constantly evolving and pertinent standards and policies may not be created or accepted in the near future. It is essential to protect sensitive information, but the overall value of this data to a verification system suggests that some risk of exposure may be worth accepting.

States should take advantage of the potential contributions of societal verification. If they do not, they risk losing the opportunity to significantly strengthen arms control and non-proliferation treaty verification.

Working Group participants identified areas of critical need to advance the concept of societal verification for nuclear threat reduction. These recommendations include actions for government officials and policy makers, technical specialists inside and outside government, and other diverse expert communities, which will move societal verification from promise to practice.

RECOMMENDATIONS

Governments need to build a foundation for societal verification within the current arms control policy leadership. They should develop policies, diplomatic guidance, and bureaucratic structures to evaluate and integrate societal verification data in treaty verification. To take advantage of new tools and techniques, governments should:

- Map out an effective process for societal verification data integration and program management to support future verification systems and begin to address questions such as:
  - Which agency has the lead?
  - How will the effort intersect with the private sector, the intelligence community, and other potential contributors?

    – How can conclusions be validated using inputs from traditional verification tools?

- Begin international consultations on how future arms reduction agreements may acknowledge and develop rules for the use of societal verification data.
- Explore the possibility of experimenting with cooperative societal verification measures with allies to provide empirical data and lessons for how societal verification may be implemented in the future.
- Start developing rules related to the legal, ethical, and privacy concerns surrounding use of citizen-generated information.

The international technology and policy community should collaborate to develop a technology needs assessment/research and development roadmap to build capacity within government systems. Areas of exploration might include the following:

- Natural language processing of foreign languages as well as informal and unstructured language, such as slang and terms of art.
- Challenges posed by real-time processing of data versus queries of stored information.
- Identifying key or leading indicators of treaty-proscribed activities around which appropriate queries can be developed.
- Identifying attempts to censor or spoof data, especially where there is knowledge that information is being analyzed.
- Aggregating and integrating signals from multiple sources across platforms and data types to increase confidence.

Governments, in cooperation with outside expert communities, should establish channels to elicit the input of outside analysts to help build approaches for societal verification as follows:

- Assess capacity and fill gaps to enable contributions by outside experts to societal verification efforts of governments.
- Develop methods and mechanisms to educate expert communities outside the government on existing national verification efforts.
- Develop ways to identify, connect, organize, guide, assist, and reward experts, recognizing that validation and anonymity are not always compatible.
- Create paths to solicit input in a timely manner on potential verification challenges.
- Encourage discussions and cross-checking among external experts, facilitating a two-way information flow to build valuable capacity outside government.

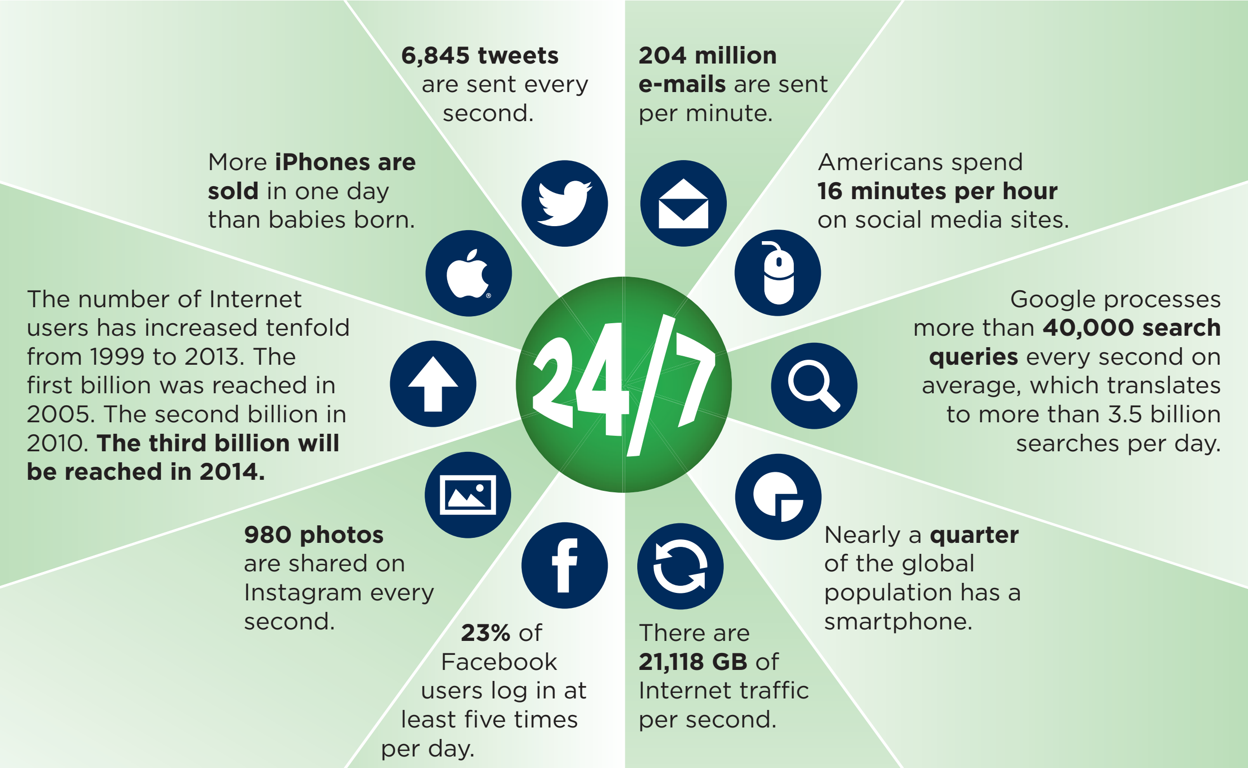
2. Introduction

Information and communication technologies (ICT) have reshaped how countries, corporations, and private citizens share, collect, and analyze information. The Internet is the bedrock of this transformation, connecting more people and devices than ever before. A Council on Foreign Relations task force on Internet governance estimated that by the end of this decade, some 6 billion people will be online, and as many as 31 billion devices could be connected to the Internet.[1]

The dramatic growth in Internet use has precipitated a boom in new media tools. Within a decade of the World Wide Web being proposed, blogs, personal websites, e-mail, instant messaging services, search engines, and peer-to-peer file sharing emerged as popular web functions. By 1999, there were 70 million computers connected to the Internet. In the 2000s, social media sites boomed with the arrival of new social networking sites such as LinkedIn, MySpace, Facebook, Flickr, YouTube, and Twitter. By 2012, there were more than 1 billion users on Facebook, 500 million Twitter users, and 400 million Google+ users.[2] See Figure 1 for an illustration of the volume and scale of online activity.

The characteristics of Internet traffic are changing as the scale rapidly expands. In 2012, 26 percent of Internet traffic originated from mobile devices, such as smartphones and tablets. This share is expected to grow to 49 percent by 2017.[3] Much of the growth in mobile-originated traffic is due to the global expansion of smartphone technology. The International Data Corporation (IDC) forecasts that by the end of 2017, smartphones will account for more than two-thirds of total mobile phone shipments, driven primarily by falling costs of technology, wider smartphone strata, and the global increase in fourth-generation (4G) wireless networks.[4] While mature economies have driven the global growth in smartphones, IDC forecasts that populous countries with growing economies, such as China, Brazil, and India, will account for an increasing share of the global demand. In 2012, China surpassed the United States as the world's largest market for smartphones.[5]

Figure 1: Global Scale of Online Activity



6,845 tweets are sent every second.

204 million e-mails are sent per minute.

More **iPhones are sold** in one day than babies born.

Americans spend **16 minutes per hour** on social media sites.

The number of Internet users has increased tenfold from 1999 to 2013. The first billion was reached in 2005. The second billion in 2010. **The third billion will be reached in 2014.**

Google processes more than **40,000 search queries** every second on average, which translates to more than 3.5 billion searches per day.

980 photos are shared on Instagram every second.

Nearly a **quarter** of the global population has a smartphone.

23% of Facebook users log in at least five times per day.

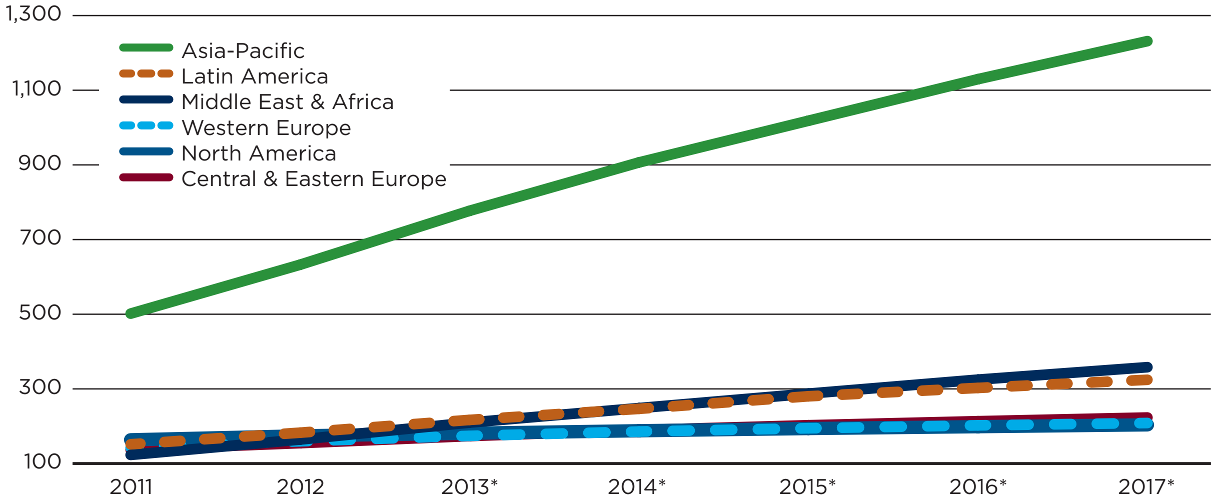
There are **21,118 GB** of Internet traffic per second.

Sources:
Internet Live Stats, http://www.internetlivestats.com/
Search Engine Journal, 2013, http://www.searchenginejournal.com/growth-social-media-2-0-infographic/77055/
Intel, 2012, http://scoop.intel.com/what-happens-in-an-internet-minute/
eMarketer, December 2013, http://www.emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536
Luke Wroblewski, "Data Monday: Mobile Devices Per Day," May 2013, http://www.lukew.com/ff/entry.asp?1728.

As global communication technologies have increased, so too has the amount of publicly generated data. The big data phenomenon has led to groundbreaking innovations in emergency response, humanitarian relief, disease control, and commercial marketing and sparked interest in the domains of nuclear arms control and non-proliferation. This information revolution has drastically affected how the public might contribute to future arms control verification efforts.

This report redefines societal verification as the process by which states or international organizations use information generated by individuals or expert communities for arms control or non-proliferation treaty verification. Early approaches, starting in the 1950s (see "Societal Verification: What's in a Name?"), envisioned the use of public mobilization to report violations in the face of limited abilities to detect clandestine weapons programs. Under that vision, the citizens of a country under a disarmament

Figure 2: Social Network Users Worldwide, by Region (in millions)



*projected

Source: eMarketer, "Social Networking Reaches Nearly One in Four Around the World," June 18, 2013, accessed September 25, 2013, www.emarketer.com/Article/Social-Networking-Reaches-Nearly-One-Four-Around-World/1009976.

The Asia-Pacific region is projected to have the most growth in social network users over the time period.

agreement could be tasked with the responsibility to report violations to strengthen inspection efforts.[6]

As satellites and other forms of national technical means (NTM) emerged, enthusiasm for societal verification faded but was revived in the 1990s in anticipation of future verification needs and newly available tools. In 1992, Joseph Rotblat defined societal verification as "a system of monitoring compliance with treaties, and detecting attempts to violate them, by means other than technological verification … based on the involvement of the whole community, or broad groups of it."[7] He underscored the difference between national verification efforts and societal verification, and recognized the need for public involvement. His concept focused on collaboration between governments and the public and is reflected in more modern definitions that describe "ways in which social actors and social activities can collectively contribute to the verification of arms control agreements"[8] and "the involvement of civil society in monitoring national compliance with, and overall implementation of, international treaties or agreements."[9]

Arms control verification has relied almost exclusively on tools such as on-site inspections and satellite imagery. U.S. and Russian inspectors have a deep reservoir of expertise after more than 20 years of conducting on-site inspections and data exchanges, but future international verification needs will require an increasingly diverse set of

SOCIETAL VERIFICATION: WHAT'S IN A NAME?

The concept of societal verification has evolved significantly in recent years, so much so that some have questioned whether the term is outdated and should be dropped in favor of another description for the kinds of activities that are the subject of this report. The challenge is that alternate phrases are either inaccurate, or do not fully explain how the information revolution can contribute to verification. For better or worse, the term *societal verification* evokes two key concepts that are appropriate for non-proliferation and arms control treaty implementation: namely, that society has a role in generating and analyzing information and it can contribute to the verification of a specific set of commitments rather than general snooping or whistleblowing by citizens on their own (or other) governments. Some alternatives to the term have appeal but do not fully capture the vision and application of the concept fully. These options include the following:

- **Inspection by the people.** In the 1950s, Seymour Melman and Lewis Bohn introduced this concept, based on the idea that the general public supported nuclear disarmament and would participate in arms control, not only out of interest, but out of a sense of moral obligation. They encouraged citizens to place international concerns over domestic loyalties by reporting violations and proposed that disarmament agreements require participating governments to develop assurances and protection for individuals reporting on their country's activities. Because this concept relies almost exclusively on whistleblowing, it does not accurately reflect that governments ultimately make compliance determinations. It also fails to account for what has changed in the past 60 years with the vast amount and variety of information now generated by the public.

- **Public technical means.** This term has appeal because it parallels the concept of national technical means, which refers to information generated and controlled by state-owned hardware systems (such as satellites) and other intelligence sources and methods. The concept of public technical means, however, envisions a set of tools dispersed widely for collection of real-time data that might have arms control or non-proliferation significance. This tool set is largely sensor driven and thus more narrowly focused than some other concepts. While sensor data could be a valuable part of a future societal verification system, other assets also need to be taken into account. In addition, most data individuals generate are not a public resource. The information is often privately owned and accessed by permission only, and access can be denied for any or no reason. This gatekeeping means that the information may be vulnerable to economic factors, commercial considerations, and corporate politics and might not be able to be relied on for uninterrupted treaty monitoring.

- **Big data, information analysis technologies, social media analytics.** These terms describe the information and tools that might be used, but not the overarching concept or process through which their content is acquired, analyzed, or applied. These tools and data form the foundations of the societal verification concept, but do not adequately explain who would use the information and how it could help verify agreements. The terms capture the what, but not the who or how of societal verification.

capabilities and tools. As most strategic arms control verification has occurred bilaterally, countries have no experience verifying multilateral agreements through direct on-site inspections by states parties. Multilateral regimes such as the Chemical Weapons Convention (CWC) and the Nuclear Non-Proliferation Treaty (NPT) use inspections conducted by international implementing bodies such as the Organization for the Prevention of the Chemical Weapons (OPCW) and the International Atomic Energy Agency (IAEA). Multilateral arms reductions agreements will likely require different approaches and new tools as more players are brought in.

Through societal verification, states can leverage new technologies and publicly available data to supplement NTM and other traditional verification methods. As information collection, analysis, and promulgation technologies continue to evolve and perform increasingly diverse functions, societal verification can increase the likelihood that violations of international commitments are detected. Societal verification might also help strengthen the connection between non-proliferation and arms control objectives, two currently distinct realms that will be increasingly interconnected as states move toward eliminating nuclear weapons while continuing nuclear power programs.

In recent years, the core tenets of societal verification have evolved further as a result of the widespread growth in technology and big data domains. The modern concept in this report is based on collaboration between governments and their citizens. While some skepticism is warranted, failure to use information in the public domain could make governments less effective and stifle key indicators of destabilizing activities. Societal verification can help build confidence among citizens, their governments, and those not party to specific arms reduction agreements, including states without nuclear weapons.

As open-source technologies create a means for stronger public role in verification, however, it is not yet clear how the information can and should feed into national systems, raising moral, ethical, and legal questions for serious examination. Given these questions, the use of data analytics or crowdsourcing will likely not push the envelope for arms control and disarmament. Communities addressing topics such as climate change and disaster relief, with less need for, and tradition of, state secrecy, are more likely to take the lead in employing society-derived information and other open sources of data. However, the arms control community needs to be fully aware of emerging norms in this area to realize the advantages that such tools offer for future arms control and disarmament initiatives.* The fundamental question remains as to whether societal verification is additive or transformative.

* There are already examples that can inform arms control verification where data collected for one purpose (e.g., environmental violations, disease monitoring, antipoaching campaigns, etc.) have revealed something else. Global Green was created to look at the environmental effects of Russia's actions to destroy its weapons of mass destruction (WMDs). It has expanded to become a global non-profit organization advocating the destruction of its WMDs.

BASIC DEFINITIONS

The term *compliance* refers to the act of meeting one's obligations. Two related but distinctly different terms, *monitoring* and *verification*, are frequently confused in arms control discussions. In the arms control and disarmament context, monitoring is the process of gathering facts that serve as evidence regarding whether a party to a treaty or other agreement is complying with the obligations it undertook. Verification refers to ascertaining the truth or reality of something. It requires looking beyond words to deeds. In the arms control and disarmament context, verification is the process of evaluating all available information, establishing what the treaty obligation is, and then determining whether a party has complied with its obligations under an arms control treaty or agreement.

Monitoring

Monitoring is a technical process involving the gathering of information through national technical means, including satellite imagery, radar surveillance, seismic instrumentation, atmospheric and soil sampling, and electronic surveillance, as well as through cooperative mechanisms established by the agreement, such as on-site inspections, remote video streaming, chemical sampling, and the use of various sensors. Cooperative monitoring mechanisms are tailored to the specific limits and requirements contained in an agreement. Information collected through intelligence gathering may also contribute to the determination of whether a treaty's limits and obligations are being met, but intelligence gathering frequently targets the acquisition of information that goes beyond what is necessary to assess treaty compliance.

Raw monitoring data is subjected to a significant amount of analysis. Vast amounts of information must be reviewed for relevance, reliability, and accuracy. Information from multiple sources is collated to assist in resolving any ambiguities. Rarely is monitoring data 100 percent conclusive. In compliance monitoring, some level of uncertainty is to be expected.

Verification

Verification is not a technical process; it is a political process, requiring a clear determination of what a treaty requires, coupled with an assessment of information collected by monitoring systems and refined by analysis to conclude whether treaty obligations are being satisfied. If the obligations in the treaty are not clear as to what constitutes a violation, or if uncertainties regarding the monitored parameters and activities cannot be resolved, compliance decisions become judgment calls. The significance of the potential violation and the security risk that such a violation entails must be considered when making compliance judgments. In some cases, direct observation of compliance with an arms control provision may not be possible for safety or security reasons. However, inferences may often be drawn by observing related functions, equipment, or parameters.

Inevitably, verification relies to some extent upon deductions of the intentions and behavior of treaty partners as well as interpretations of the evidence. Non-compliance can result from a variety of circumstances. An accident, oversight, or unauthorized action could lead to an inadvertent violation of an agreement's technical requirements. Ambiguity in the language of the agreement or a misunderstanding between the parties on a point of interpretation could lead to a finding of non-compliance. There could be deliberate minor incursions of an agreement's restrictions in a conscious attempt to test the limits of the other party's monitoring capabilities. Finally, a party could engage in a deliberate and massive violation intended to gain a military or political advantage. The response to such different non-compliance situations needs to account for the motivations of the violator.

The verification process must be sufficiently robust to permit a party timely warning whenever treaty breakout, or a threat to national security, is imminent. The consequences related to a violation being identified and the threat of detecting such a violation must be significant enough to deter violations. Regardless of how strong a monitoring regime may be, if provisions can be violated with impunity, there will be no deterrent effect. Similarly, if the chances of detecting cheating are slim, violations may occur even when the consequences of detection are severe. Militarily insignificant violations of a treaty or agreement can erode confidence in the ability of arms control agreements to enhance security and stability.

A comprehensive monitoring and verification regime should account for every provision of a treaty containing an obligation. If obligations do not matter enough for the monitoring system to address them, they should not be enshrined in the treaty. Otherwise, compliance will be indeterminate and confidence will erode. However, no matter how comprehensive a monitoring regime may be, it is always possible that violations could go undetected. A monitoring regime that is comprehensive and effectively tailored to the clearly articulated, concrete obligations in an agreement stands a better chance of identifying compliance concerns. Such a monitoring regime, coupled with an extensive verification process, can significantly deter cheating and provide confidence that major treaty violations will be identified in a timely manner so that the potential military advantage of the violations can be countered and a stable security relationship maintained.

International organizations and monitoring systems can provide useful input to states attempting to make verification assessments, but ultimately individual parties to an agreement are responsible for their own compliance determinations. While international organizations such as the International Atomic Energy Agency can conduct inspections, collect data, and employ cooperative measures to great effect, their data gathering is constrained to agreed measures.

3. Transformative Information Technologies: Lessons Learned

The challenges facing societal verification are not unlike those created by other groundbreaking or disruptive technologies. Throughout history, technology has constantly evolved and been used in new and innovative ways. When the telegraph, radio, and commercial satellite imagery were first introduced, governments and their citizens greeted them with skepticism and reluctance. Since then, they have profoundly affected how policymakers and the public communicate and solve problems, creating more expedient platforms for conducting diplomacy and analyzing national and transnational activities.

TELEGRAPHY

Telegraphy grew from electrical experiments in the late 18th century, when observers noted that electricity flowing between a negatively and positively charged point could be seen as a type of signal.[10] From there, developments followed rapidly, leading to the invention of the first practical telegraphs in England and the United States in the 1830s. Telegraphy rose to prominence in the mid-19th century through the initial influx of significant funds from the U.S. government to Samuel F.B. Morse in 1843. Those government funds made the first practical public demonstration possible in 1844, with the transmission of a message between Washington D.C. and Baltimore: "What hath God wrought!"[11] The first successful transatlantic telegraph cable was completed in 1866.[12]

The telegraph was a transformative telecommunications medium with wide-ranging and global effects on governmental operations and life in general.[13] Point-to-point telecommunication was a quantum leap over previous methods of communication, which were limited to either surface transport for long distances or semaphore (using flags). People at the time correctly anticipated that telegraphy would significantly accelerate communications, and hence, the pace of diplomacy. This, in turn, increased the demand for faster access to information, particularly among financial speculators and journalists. Ministries centralized authority in capitals, diminishing the role of diplomats to personally carry messages. The medium encouraged concision and succinctness, rather than the previously more flowery and verbose diplomatic language. Finally, states had to invest in infrastructure and recruit and train skilled telegraphers.

Telegraphy also produced a number of unanticipated effects. The fast pace of communications left less time for reflective decisionmaking and increased pressure on policy makers. Bureaucracies experienced heavier workloads because of round-the-clock shifts to receive telegrams and increased activity during crises when normal prohibitions against using the telegraph disappeared. The process of coding, decoding, and otherwise handling telegrams was very time consuming. Challenges to using the incoming information included authenticating messages; developing countermeasures, such as encryption and codebreaking; and managing garbled or incomprehensible messages. Yet telegraphy was rapidly adopted and maintained prominence well into the early 20th century, until it was surpassed by the invention of the telephone.

National systems and institutions often adapt to new technology at a slower rate than anticipated. It may take time to incorporate societal verification into existing systems.

RADIO

"The Wireless Music box has no imaginable commercial value. Who would pay for a message sent to nobody in particular?" associates asked David Sarnoff, pioneer of the radio and television industry, in response to his urgings for investment in radio in the 1920s.[14] Developed as a "single point-to-multipoint" transmission medium, radio technology had its roots in 18th-century advancements in telegraphy. Building on Heinrich Hertz's work on electromagnetic waves, inventors competed with each other to develop wireless telegraphy, and in 1897 Guglielmo Marconi patented the first successful radio transmitter.

The adoption and spread of radio technology has at least four important lessons for societal verification today. First, the government can play an important catalytic role. Just as the U.S. Department of Defense pioneered the Internet, the U.S. military first recognized the utility of the radio and began to incorporate the technology into its operations, using radio transmitters as navigation aids and supplementing nascent commercial stations whenever necessary. With the U.S. entry into World War I, the Navy assumed total control of the radio station network. After the war, the Navy argued forcefully to maintain its monopoly, and private radio stations were again legalized only after Congress intervened.[15]

Second, regulation is key. Although it took time for the entertainment value of radio to catch on, the public safety role was quickly recognized. The *Titanic* had a radio room on board and was able to transmit a distress signal to the nearby *Carpathia*, which immediately sailed to assist with the rescue effort. However, radio's role in the rescue was marred by reports of interference from numerous amateur operators in the New York area eager to share news of the event.[16] The true extent of the interference was disputed, but outrage over the incident led Congress to pass the Federal Radio Act of 1912, the first U.S. government effort to regulate the airwaves.[17]

Third, technology can be used to spread important messages, unfiltered by the news media or others. The relevant lesson for new media may be found in one of the most successful government uses of radio: President Franklin Roosevelt's Depression-era "fireside chats." For the first time, a president could take his arguments directly to the people without the filter of the press. The resulting flood of positive listener letters was then used as evidence in support of his programs.[18] Germany and the Soviet Union employed the same technology to vastly different effect.[19] Later, both the United States and the Soviet Union used radio in large-scale information campaigns. Although the goal of spreading democracy is laudable, this public effort has been wrapped in controversy and legal complications.[20] Moreover, Radio Free Europe's connection with the Central Intelligence Agency (CIA) until 1974 continues to surface in foreign press articles, demonstrating the difficulty of shedding any intelligence association once it has been established.

Finally, national systems and institutions often adapt to new technology at a much slower rate than anticipated. Although 60 percent of U.S. homes had a radio by 1934,[21] a widely accepted theory of mass media communication was not developed and articulated until Elihu Katz's idea of the two-step flow of communication in 1955.[22] As the ongoing debate over public broadcasting funding, the fairness doctrine, and equal time rules demonstrates, the government's proper role in and appropriate use of radio is still being explored today. This shows that it may take time to incorporate societal verification into existing systems, and such information may not be immediately and confidently reliable, but it can still play a significant role.

COMMERCIAL HIGH-RESOLUTION SATELLITE IMAGERY

Commercial satellite imagery was an outgrowth of Cold War–developed and satellite-based national technical means (NTM) technologies that first proved the concept of remote sensing from space. While early NTM systems were based on analog (film) cameras, now commercial satellite imagery is entirely digital. Space-based orbital systems provide a non-intrusive means of remote sensing and an inherent capability to directly obtain information about otherwise inaccessible areas anywhere on earth with predicable regularity. Commercial satellite imagery differs significantly from both telegraphy and radio in that it serves only as an information data source rather than a means of information transmission. In addition, it generally requires the specialized expertise of trained imagery analysts to extract accurate and complete information. Initially, there was strong skepticism regarding quality, cost, timeliness of acquisition and delivery, and potential vulnerability to countermeasures such as moving activity under cover.

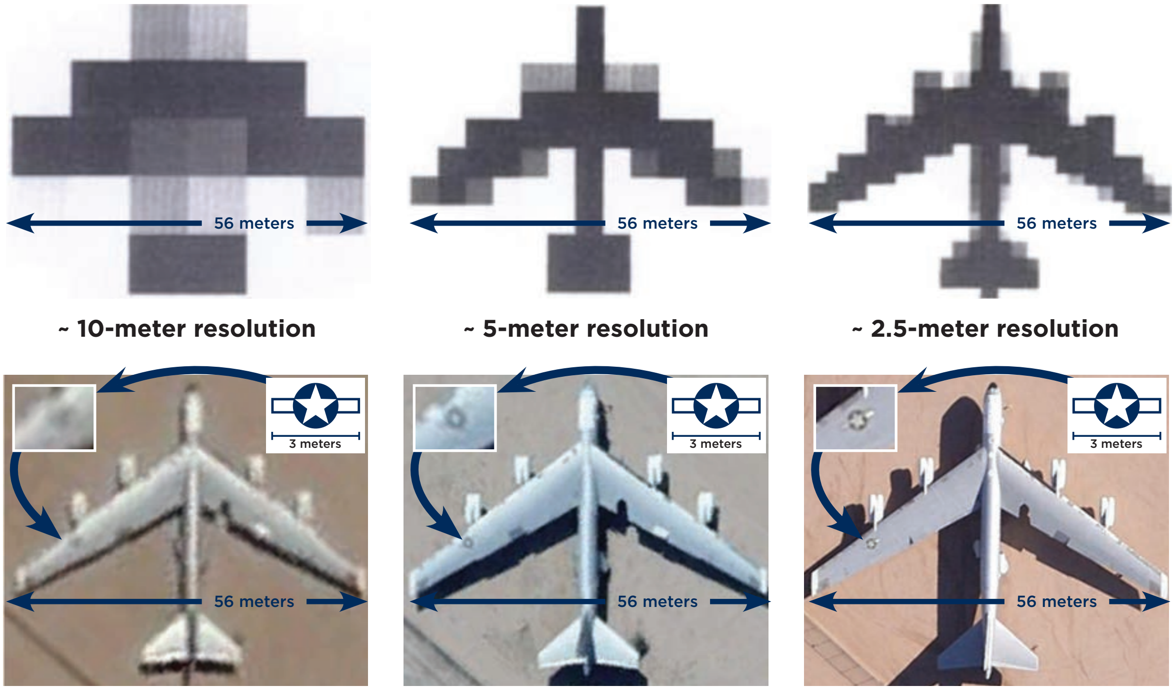
Remote sensing was first made possible with a combination of improvements to cameras and the ability to place cameras in balloons, on kites, and even on large pigeons. By the beginning of the 20th century, propelled aircraft were the most reliable means of aerial-based remote sensing. With the dawn of the Space Age in the late 1950s, cameras could be placed in earth's orbit to remotely and routinely image any point on the globe.

The first publicly accessible imagery from space was available through the civilian U.S. Landsat system beginning in 1972. The Landsat-1 satellite carried digital scanning sensors that covered four multispectral bands, providing color-composite coverage of the earth, but it was essentially useless for any substantive verification applications given its resolution of 80 meters per pixel. In early 1986, however, France's SPOT-1 (Système Pour l'Observation de la Terre) became the first commercial imaging satellite to provide the public with imagery of sufficient resolution and quality to have the potential for verification applications. Images from the SPOT-1 satellite and the improved Landsat-5 provided the first publicly available visible evidence of the Chernobyl reactor disaster in Ukraine in April 1986[23] and profoundly influenced public perception and international response.[24] Shortly thereafter, researchers began to publish on potential uses of satellite imagery, its benefits, and its expected drawbacks.[25]

By the early 1990s, researchers correctly anticipated that commercial satellite imagery would contribute to public debates about arms control and non-proliferation issues. Many also argued that commercial satellite imagery would support cross-border conflict monitoring, multilateral peacekeeping, crisis decisionmaking, and treaty verification and monitoring. The capability facilitated competition with official national intelligence reporting, making it possible for non-governmental experts to publicly assess proliferation and security concerns and serve as a check on the conclusions that governments made. It also led to arguments about quality of data and analysis, cost, timeliness, and censorship—all issues that are currently discussed in the context of societal verification. Some states and corporate entities have responded by pursuing countermeasures such as camouflage and deception. As commercial satellite imagery has become more widespread, it also has caused more mistaken interpretations, particularly by inadequately trained imagery analysts.

Today, commercial satellite imagery resolution is accessible at 50-centimeter resolution from multiple satellites, and if U.S. law changes, imagery of 25-centimeter resolution will soon be available (see Figure 3). Thanks to wi-fi, rapid file transfer protocol (FTP) rates, and smart phones, high-resolution imagery is now freely available and accessible practically anywhere. Digital virtual globes such as Google Earth have been

Figure 3: Effect of Resolution on Overhead Imagery of B-52 Bomber



Source: Bhupendra Jasani and Gotthard Stein, *Commercial Satellite Imagery: A Tactic in Nuclear Weapon Deterrence* (New York: Springer, 2002).

Dramatically improved resolution of publicly available satellite imagery means that individuals and governments without their own spy satellites can do independent analysis.

downloaded more than 1.2 billion times and imagery is often freely available for non-governmental organizations (NGOs) to use.

Key conclusions from early analyses of satellite imagery capabilities suggested that superpowers (or any other national government or agency) would no longer be able to control the narrative regarding their programs, as commercial satellite imagery would provide democratizing access to information previously unobtainable before. The imagery would be a double-edged sword, with both positive and negative applications, but on balance the potential for good would far outweigh the potential for malice. As the imagery would not come with labels, it would require skilled interpretation to have value. Mistakes could and would be made, so corroboration by other sources would always be required. Finally, cost and timeliness would always be a concern.[26] Each of these points could be applied to the current international discussion about new media and its application to treaty verification. Just as commercial satellite imagery has tested systems, so will societal verification.

LESSONS LEARNED

Fundamentally, the greatest challenges posed by transformative technological tools have not been technical, but have involved institutions' slow reaction to them. In each of the cases above, as with societal verification, it is difficult to predict the value of technology and new data as it is emerging. But already these technologies have changed how governments and their citizens share and interact with written, verbal, and visual communications. Lessons from their development and evolution highlight the need to develop a cadre of skilled experts; the need for government rulemaking and oversight; the difficulty, once established, to shed an association with intelligence collection; the dual use—for help or harm—of the technology; the need for integration of newly produced or disseminated information and that derived from more traditional sources; and the need to prepare for the evolution of the tools and associated information over time.

4. New Media and Geospatial Tools

In late 2011, then-Assistant Secretary of State Rose Gottemoeller publicly outlined a number of near-term arms control challenges and the difficulties in monitoring controlled materials, warheads, and missiles, particularly in future arms control agreements as the quantities got smaller and more states joined the effort. She posed the question of whether "open source information technologies and social networking could contribute to arms control verification and monitoring?"[27] This question recognized that traditional national technical means (NTM) relies on an aging infrastructure that might not meet future verification requirements. There is a need to take stock of the new tools and sources of information that could be integrated into a larger system for more effective verification.

The growth of Internet-enabled technology has been accompanied by an explosion in new terms to describe the technology. Although *social media* is the most widely used, it is more accurate to refer to the entirety of these capabilities as *new media*. All new media share essential characteristics: every consumer can be a producer; the media are generally free to the consumer and sometimes to the producer; the media products both compete and act as catalysts for each other; and the underlying software platforms are beyond the control of individual users.[28] New media can therefore be understood as the broadest categorical term to describe all interactive online activities. They include a vast array of tools for information collection, dissemination, and analysis. These tools and the analytical approaches applied to them are not based on fuzzy concepts; there is real math and science applied and a growing literature to back it up.

The sheer number of new-media tools and platforms is daunting. Wikipedia lists almost 200 social networking websites in its entry on the topic. The list expands continually[29] and is far from exhaustive. Social bookmarking sites such as Reddit or Digg rely on interaction to determine the most popular reader topics but do not provide the degree of user identification associated with overt social networking sites, such as Facebook or LinkedIn. Microblogging platforms such as Twitter or Tumblr allow members to follow each other and create relatively detailed user profiles but lack the high degree of individual user-to-user interaction that characterizes typical relational networks.[30] So far, mapping or geospatial software such as Google Earth has been poorly integrated into the existing social media environment, still relying mostly on outside enthusiasts to catalog lists of interesting findings on individual user blogs or aggregator websites such as Mashable. Last, technology and public interest are constantly changing. The decline of former technology leaders, such as Myspace and Second Life, is proof that the most useful and popular platform can rapidly lose both functionality and the critical mass of user support that makes it valuable.

Identifying roles for new media in verification is best pursued by assessing how a particular type of new media will function rather than identifying and assessing specific platforms or operators. Social networking sites are just one type of new media. Others include gaming, data analysis applications, and collaboration platforms. Table 1 summarizes these categories and examples of typical platforms or operators.

Three software platforms currently enjoy widespread popularity among users and social media researchers: Facebook, Twitter, and Ushahidi. Facebook, the most popular, is a true social networking site in that it allows users to create a public profile, publish a navigable list of connections, and view and navigate the connections of others within the system.[31] These features are perhaps most applicable to societal verification. In 2012, when radioactive sources were stolen from a nuclear power plant under construction in Egypt, Facebook users publicized the theft well in advance of official media.[32] Authorities and citizens have effectively used such crowd-based reporting to identify and capture criminals.[33] Most significantly, Facebook is the only social networking site with reliable evidence of online friendships affecting offline behavior. Researchers reviewed 61 million Facebook accounts to track the ability of friends to encourage each other to vote; this friendship effect appears to be tiny, but provides some evidence for generating the type of positive collective action that could undergird societal verification efforts.[34]

The microblogging platform Twitter also has received a lot of attention. There is still considerable debate over Twitter's role in spreading information and encouraging popular protest during the Arab Spring, but few today doubt the platform's importance as a source of information and an indicator of public sentiment.[35] Twitter, however, is much closer to a traditional news outlet than a social networking site.[36] Researchers have discovered that the dynamics of Twitter usage are typical of today's media markets, with a tiny number of users exerting disproportionate influence. Popular and recognizable media companies (e.g., *The New York Times*) and celebrities (e.g., actor Ashton Kutcher) dominate the information flow on Twitter.[37] There is little evidence of Twitter's value in gathering specific intelligence information, but researchers are beginning to establish Twitter's usefulness as a sentiment index. An analysis of positive, negative, or neutral sentiments has been shown to correlate well with real-world political outcomes,[38] stock market performance,[39] and consumer confidence.[40] Sentiment could be similarly

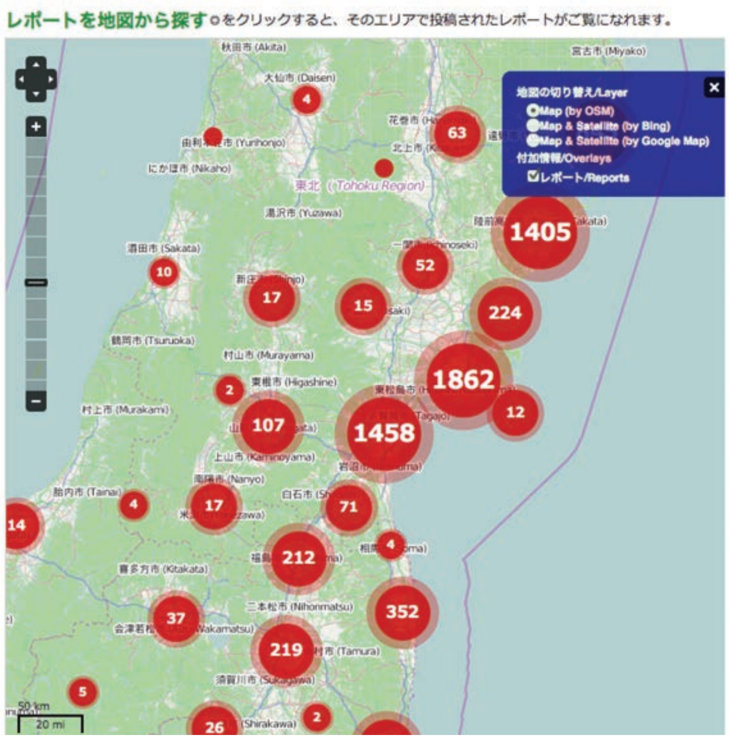
Table 1: New Media Functional Categories and Examples

Category	Example
Gaming and simulation	• Social gaming – Facebook apps – Global gaming communities (e.g., World of Warcraft) – Location-based games (e.g., Four Square) • Educational gaming • Simulations – America's Army – MS Flight Simulator
Social	• Social networking platforms – Facebook – Twitter – RenRen (China) – Sina Weibo (China) – Odnoklassniki (Russia) • Virtual communities – Reddit – Chatrooms • Communication services – E-mails – Instant messaging/texting – Video and photo sharing
Content creation/ collaboration	• Content management systems – WordPress – Tumblr – LiveJournal (Russia) – Ameblo (Japan) – Persianblog.ir (Iran) • Wikis • Crowdsourcing platforms • Crowdfunding platforms – Kickstarter • Crowd mapping platforms – Ushahidi
Data mining and processing	• Big data analysis – Palantir – Recorded Future • Graphical information systems
Problem solving/hacking	• Public Challenges – Innocentive – GitHub • Design and coding hackathons

aggregated to gauge public support for arms control treaties or sanctions regimes. While widespread, both Facebook and Twitter are majority English-language, Western, and Northern communities. Similar engagements could be facilitated in specific countries and regions using analog services such as China's Sina Weibo.[41]

The final new media tools that receive the most discussion with respect to societal verification efforts are crowdsourced mapping platforms such as Ushahidi. While geospatial enthusiasts tend to focus on the Google Earth software, non-profit interactive mapping company Ushahidi has garnered widespread attention for its efforts in mapping disaster zones and aiding relief efforts. The system allows users to submit information by a variety of means, including mobile telephones. Relief workers can easily vet and aggregate these reports to aid in rescue and recovery efforts.[42] The maps can also be integrated easily with existing remote sensors, providing a simple and effective method for citizens to plot and track disaster events. Harvard University used the Ushahidi technology to establish an earthquake map in the wake of the Fukushima disaster (see Figure 4). The publicity over Fukushima led to a surge of interest in radiation tracking, and there are now dozens of sites using mapping technology to track radiation emis-

Figure 4: Earthquake Map Created with Open-Source Ushahidi Software



レポートを地図から探す ○をクリックすると、そのエリアで投稿されたレポートがご覧になれます。

Source: http://www.sinsai.info/index.php/main.

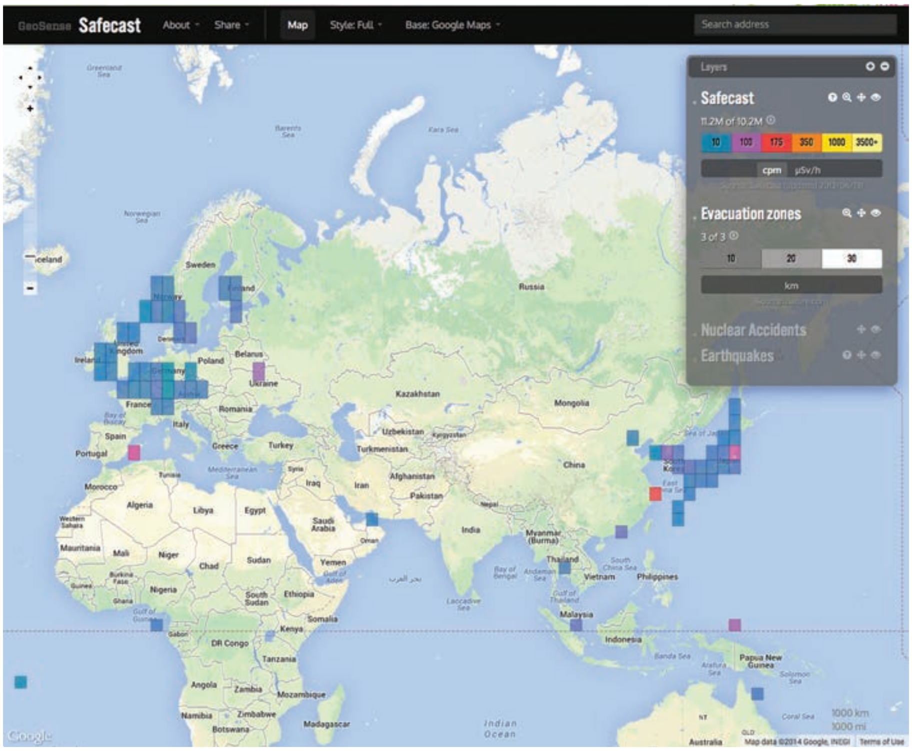
Crowd mapping and widely deployed sensors combined to create a map of earthquake activity in Japan after the 2011 Great Tohoku earthquake.

sions using public sensor networks. Safecast, a project created specifically to monitor the Fukushima event, is now the largest radiation monitoring project in the world, with a current collection of more than 4,000,000 data points (see Figure 5).[43] Such a network could provide data related to a clandestine nuclear event as the numbers and locations of sensors grows.

Many new-media platforms combine multiple functions. Kickstarter and other online crowdfunding websites are problem solving tools, as any individual with an idea for a product or service can solicit contributions from the online community. Kickstarter is also a social site, as it bonds responders into communities by interest or geography. Those who love music can fund a struggling musician to produce her first professional recording; those who love beer can fund a microbrew's business plan. Kickstarter's model may be transferable to solving other problems, such as those related to nuclear threats or non-proliferation. A technical verification tool also could be crowdfunded.

Geospatial tools are now broadly used in International Atomic Energy Agency safeguards,[44] conflict monitoring,[45] environmental monitoring,[46] and disaster assessment

Figure 5: Crowdsourced Safecast Radiation Monitoring Map

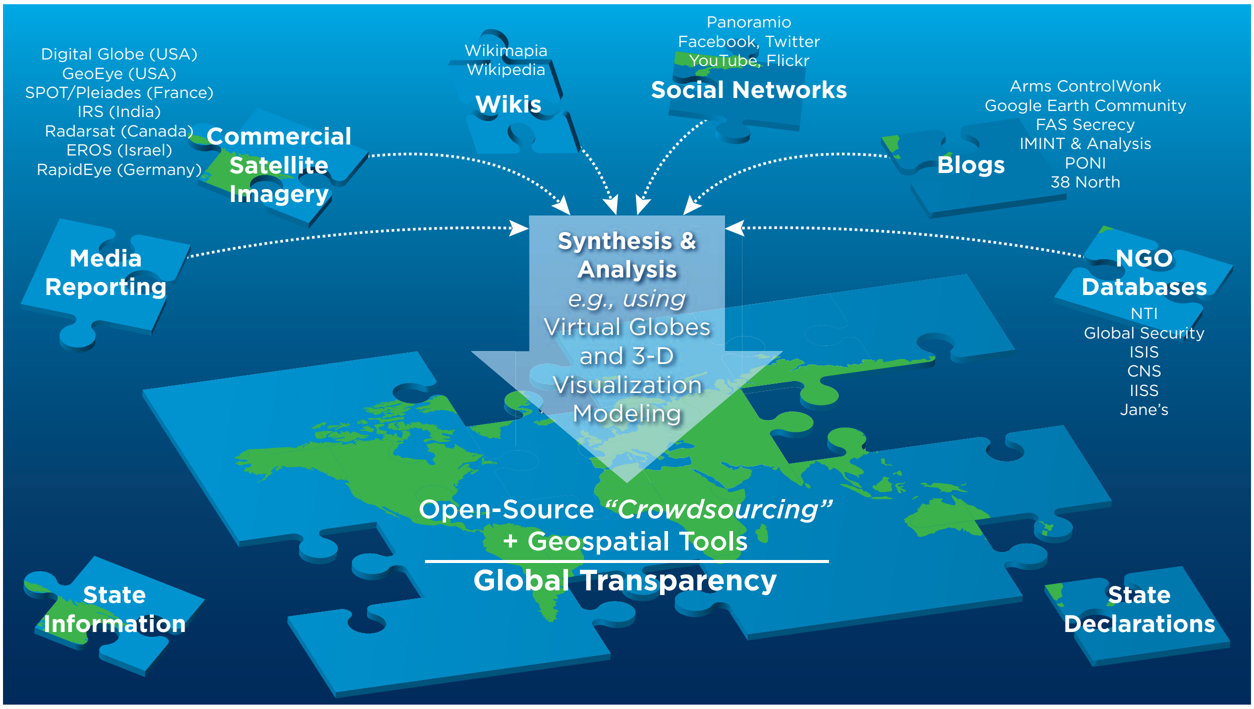


Source: http://blog.safecast.org/.

Safecast, a project created specifically to monitor the aftermath of the Fukushima nuclear event, is now the largest radiation monitoring project in the world.

(see Figure 6).[47] Publicly available, geospatially linked, ground-based imagery sharing and visualization venues[48] enable individuals to share their findings through blogs[49] and Wikis[50] and on virtual globes such as Google Earth and Google Maps. International agencies and non-governmental organizations are becoming increasingly active and adept in their use of such technologies. Actor George Clooney's Satellite Sentinel Project is currently fusing commercial satellite imagery with crowdsourced analysis and advocacy in an effort to end Sudanese genocide and crimes against humanity.[51] In the areas of arms control and nuclear security, loose groups of experts like those who blog and comment at Arms Control Wonk and 38 North routinely combine satellite imagery, news reports, photographs, official statements, and societal data to locate and characterize facilities and sites in remote or inaccessible areas, such as inside North Korea. These revelations lead to new policy insights and technical assessments of capabilities and timelines regarding weapons of mass destruction capacities.

Figure 6: Integrating Geospatial Information



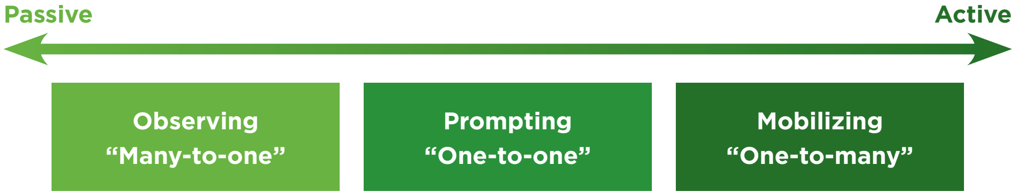
Geospatial tools, combined with publicly produced and derived information, enables independent analysis, expert collaboration, and greater transparency.

Key for Abbreviations

SPOT = Satellite for Observation of Earth
IRS = Indian Remote Sensing
EROS = Earth Resources Observation Satellite
FAS = Federation of American Scientists
IMINT = Imagery Intelligence
PONI = Project on Nuclear Issues
NTI = Nuclear Threat Initiative
ISIS = Institute for Science and International Security
CNS = James Martin Center for Nonproliferation Studies
IISS = International Institute for Strategic Studies

5. The Monitoring Continuum: Observing to Mobilizing

Societal verification could employ a diverse set of technologies and platforms for monitoring activities to ensure implementation of agreements. To use these tools, states must decide which steps are most suitable for near-term application and which require further bureaucratic, institutional, diplomatic, and technical development. One way to divide the tasks is to assess the level of engagement with the public as the data providers.



The range of interactions with and within online media mimics that of any human interaction, from passive observation to real-time communication. At the passive end of the continuum (many-to-one), online content from a large number of sources can be observed with or without triggers that focus attention on particular events or content. Many commercial platforms are suited to passive observation, such as the Tweetdeck and Hootsuite online tools for monitoring Twitter. These tools display social media content, such as the hashtags associated with tweets, and can allow a user to follow certain organizations or receive alerts when organizations, topics, or specific words are mentioned in posts. Tagboard.com expands observation abilities to include other social media sites, such as Facebook and Instagram. This sort of monitoring is real time, but requires a user to have well-defined and well-understood areas of interest, as it is a rather simple form of filtering and display.

The strength of observation is its immediacy. Real-time monitoring often provides indications of meaningful events well before other traditional sources broadcast the information. Passive observing magnifies the user's ability to see across geographical and informational expanses. This is especially crucial when information of interest may not percolate to traditional sources, may be secondary to other events, or may be gleaned from subjective expressions, such as opinions and attitudes, rather than factual information or events. Passive observing can also be effective for the surveillance of misinformation, whether intentional or inadvertent. This type of activity primarily uses common media analytics, including data mining techniques, such as sentiment analysis and topic filtering.

Further down the continuum is what might be called prompting, or one-to-one interactions, through active participation in conversations. Participation may be cued by something observed in passive observation, or initiated through a process where people are encouraged to express questions, concerns, or comments through different channels. Companies that use social media to reach out to customers increasingly employ prompting, not only to advertise, but to specifically address customers voicing complaints through social media. The methods are also good for focused questioning. Congressional testimony showed that Federal Emergency Management Agency administrator Craig Fugate asked someone in American Samoa, via Twitter, to tell him about the situation on the ground during an unfolding event.[52] Prompting is most likely to benefit from sophisticated tools that allow organizations or moderators to target questions about specific topics to specific people. Targeting could also extend to specifically identified groups of people, such as expert communities, to take advantage of a group's knowledge. This is a potentially fruitful area for societal verification, as it is likely that many of the tasks relevant to verification and transparency will require specialized knowledge.

At the farthest end of the spectrum is mobilization through the broadcast of messages with little interaction with the information receivers (one-to-many). This usage is more akin to traditional advertising and can also be paired with media analytics that evaluate how well the messages spread and influence a population.

OBSERVATION FOR SOCIETAL VERIFICATION

Broad scanning and focused data collection are two general approaches to observation that would be useful for verification. Scanning over large amounts of data often requires identifying patterns using predetermined features, such as those related to non-proliferation. The difficulties in this area are the same as those in most pattern-detection tasks; the costs associated with false positives and false negatives should be an important consideration, especially when tasks require human judgment. Analyzing large numbers of false positives could be labor intensive if it requires a person to resolve each alarm. To successfully apply large-scale data scanning approaches, it will be necessary to develop social data–based proliferation indicators, determine how those indicators would appear in social data, and collect specific data sets in a timely manner.

Some citizen reporting concepts depend on the use of personal technology, such as cell phones, cameras, computers, accelerometers, global positioning equipment, and accurate timepieces. The capabilities such technologies afford are not uniformly distributed around the world, and the distribution of privately owned technology does not directly coincide with the locations where possible treaty or agreement violations could occur. A large volume of reporting would come from population centers, while remote locations might be of most interest in treaty monitoring.

Many useful data sets are dispersed across archipelagos of obscure websites. Such data sets only become useful as they are collected and collated. The Internet as we know it could not exist without an infrastructure to perform this task; it is why search engines such as Google have been so crucial to the Internet's development. Such search engines deploy web crawlers that travel the web and catalogue websites. The resulting map of the Internet enables web searches. More targeted versions of this basic approach have also been implemented, some directly relevant to verification. The United States Geological Survey employs a web crawler that finds publicly accessible sites reporting seismic sensor data around the world and creates an interface to make this data accessible and meaningful. The previously mentioned public sites that track radiation emissions, such as Safecast, have provided a similar function. An indirect application of this approach includes maps that use cell phone data to track traffic speeds on a road network.

The strength of observation is its immediacy, providing indications of meaningful events well before other traditional sources broadcast it. This is especially crucial when information may not percolate to traditional sources.

In a slightly different approach, some programs use volunteer crowdsourcing to push data to a central location where it is transformed into usable information. Ushahidi allows the public—including activists and news organizations—to collect and use disparate information sets embedded in a geospatial database.[53] Waze uses crowdsourced traffic data collection to populate a navigation program with real-time information on traffic flows, incidents, and other information useful to drivers, such as gas prices and traffic enforcement activities.[54] The city of Boston is developing a smartphone app that uses data from the motion sensors in smart phones to locate potholes.[55] A company called GammaPix has developed a smartphone app that uses the built-in camera as a radiation detector.[56] This kind of tool could prove useful for nuclear verification in the future if its data were collected and incorporated into a national or international system.

Focusing Data Analysis

Focused data collection centers on gathering information that has already been created about specific events or entities of interest. First, an analyst must determine what kind of information is useful—type, platform, geography—and create a data query to cull the data. This process often involves collecting and analyzing co-occurring features that are paired with the topic. An analyst might track sentiment around the ratification of a

SOCIAL MEDIA ANALYTICS: STATE-OF-THE-ART CAPABILITIES

Current research in social media analytics tends to focus on three main domains: content analysis, group and network analysis, and prediction of real-world events. Content analysis consists of determining the topics, themes, and sentiments of a dataset, and determining how those change over time. New research into content analysis expands the traditional approaches from textual data sources to include social multimedia such as photos, videos, and maps. Group or network analysis is the capability of researchers to identify and describe users within a group, characterize how group members interact with each other, and identify influential users with the group. Prediction analytics utilizes social media indicators to predict future, real-world events such as movie revenues or financial market activity using a combination of the scale of social media coverage, sentiment analysis, and influence analysis.

Challenges

Social media analytics face many of the same challenges as other open-source information analytics research—mainly accessing, storing, and processing information; verifying sources and dealing with misinformation and deception; and fusing various types of data. In addition to those issues, social media research faces some unique challenges. Analytic workflows, methods, and tools have not been designed to incorporate these dynamic, massive datasets. Current researchers are dealing with the cost and infrastructure required to store and process large amounts of social media data, along with legal considerations for social media data storage. Despite the availability of social media data, there has been little work done in the area of fusing multiple types of social media data and more traditional data into one analytic environment. Finally, the use of social media data needs to be tailored according to how people use social media, the characteristics of the information available through social media, and how that information might be meaningfully utilized to answer relevant questions.

Cutting-Edge Development and Forecast for Social Media Analytics

The goal of social media analytics is continuous, automated analysis of publicly available data to anticipate and detect significant societal events, such as civil unrest, election outcomes, infectious human illness, and economic events. The ultimate goal is the automated collection, fusion, and prediction of these types of events running at massive scale without the need for human analyst intervention. Key challenges encountered within this activity to date include robust and efficient extraction of indicators from massive volumes of heterogeneous data; large-scale time series analysis of noisy, non-stationary data; learning from sparse training data; localization of models for cultural context; integration of domain-specific information; alias and word disambiguation; and integration of data-driven and model-driven methods.

non-proliferation or arms control agreement or might look for specific social data following a non-proliferation speech, policy decision, or other event. The purpose would be to review the vast ocean of available data and identify relevant activities governed by a specific set of treaty obligations. The key to successful focused data analysis is to design the right query. Examples of effective filters for such information include the following:

- **Topic or theme.** Topic identification—or the related topic modeling—is an information analytics capability often applied to social media data. It is used to categorize topics, primarily through a machine learning approach to natural language processing (NLP).[57] One example would be detecting non-proliferation topics, such as the Comprehensive Test Ban Treaty, in conversation. Topic or theme identification may be able to disambiguate discussions by determining what social media users are referring to when they are discussing that treaty: the International Monitoring System (IMS), ratification of the treaty, or the use of Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO) data (seismic, hydroacoustic) for scientific research.
- **Sentiment.** Sentiment analysis uses predefined dictionaries to determine the sentiment—generally positive, neutral, or negative—of a statement.[58] Active research is focused on determining additional dimensions, such as energy level[59] and more complex human emotions.[60] Sentiment analysis, when paired with topic tracking, may be able to assess a specific population following a significant non-proliferation or arms control event; however, caution should be used as it is likely that some sentiments are more often shared than others, resulting in a biased sample.[61] Sentiment analysis could provide additional information about whether reaction to a nuclear test was positive (supporting the test), negative (condemning the test), or neutral (reporting news of the event). Several nuances of language, including sarcasm, regional differences in English, and cultural nuances, make sentiment analysis difficult.
- **Identification of groups and characterization of users.** A primary topic in the field of social networking analysis (SNA) is community detection, or the identification of groups. This can include direct relationships, such as Twitter followers or Facebook friends, but also relationships through common activity, such as commenting or posting on common online resources. Online community research analyzes the strength or weakness of relationships between group members and the effects of those ties on the dissemination of information through social networks.[62] Identification of groups can be used to identify individuals with common interests, such as those who comment on or contribute to the non-proliferation blog Arms Control Wonk.[63] Tracking specific groups over time may provide multiple insights, including event detection and influence patterns.

SNA can also define multiple types of ties between individuals in a social network. These ties may represent relationships, communication patterns, or temporal events. The ties

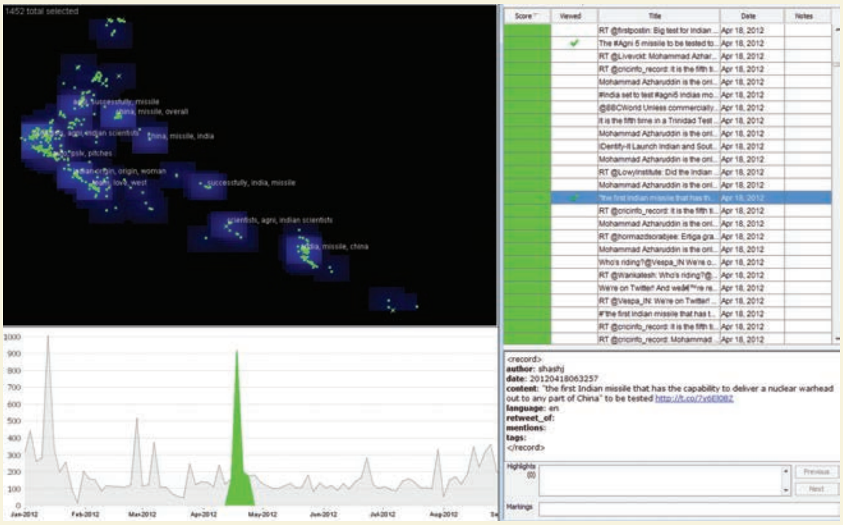
DATA VISUALIZATION

Visual analytics are tools and techniques that allow analysts to ask questions of a dataset, and receive responses in visual form. They "play off the idea that the brain is more attracted to and able to process dynamic images than long lists of numbers. But the goal of information visualization is not simply to represent millions of bits of data as illustrations. It is to prompt visceral comprehension, moments of insight that make viewers want to learn more."[65] Visual analytics can help analysts understand trends, patterns, or themes in big datasets, which they can then use to focus their data collection or revise an analytics question.

Visual analytics can show themes and topics, clustering documents by relevance; show changes in terms, themes, and topics over time; display the results of sentiment analysis over a group of documents, arranged by time, topic, and other factors; and display groups, connections, and networks from link analysis. Visual analytics can be used to help answer questions about the major topics in a dataset and changes in the presence of a given topic over time and how it is portrayed in the dataset. It can also shed light on how closely connected the authors are to information about a given topic and whether they are in the same social or professional networks.

Visual analytics are meant for use by analysts working on a problem, rather than for decisionmakers. However, the results from visual analytics may be described in a report with selected screenshots that would be appropriate for decisionmakers and policymakers. Using data visualization to communicate results is usually referred to as *information visualization* and is meant for communication purposes, giving quick understanding of information. The products are often called infographics.

Visual Analytics of the "India Missile" Dataset



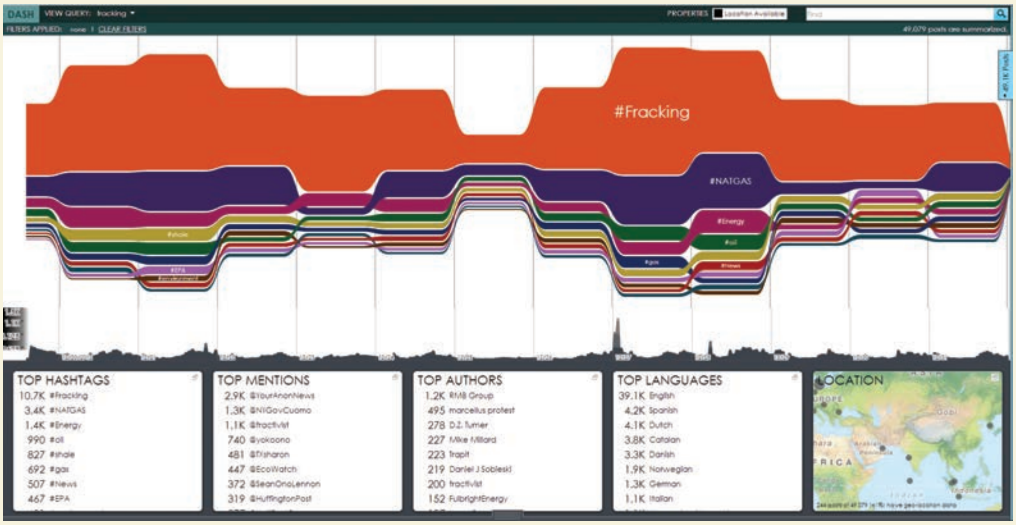
Score	Viewed	Title	Date	Notes
🟩		RT @firstpostin: Big test for Indian ...	Apr 18, 2012	
🟩	✓	The #Agni 5 missile to be tested to...	Apr 18, 2012	
🟩		RT @Livevckt: Mohammad Azhar...	Apr 18, 2012	
🟩		RT @cricinfo_record: It is the fifth ti...	Apr 18, 2012	
🟩		Mohammad Azharuddin is the onl...	Apr 18, 2012	
🟩		#India set to test #agni5 indias mo...	Apr 18, 2012	
🟩		@BBCWorld Unless commercially...	Apr 18, 2012	
🟩		It is the fifth time in a Trinidad Test ...	Apr 18, 2012	
🟩		Mohammad Azharuddin is the onl...	Apr 18, 2012	
🟩		IDentify-It Launch Indian and Sout...	Apr 18, 2012	
🟩		Mohammad Azharuddin is the onl...	Apr 18, 2012	
🟩		RT @LowyInstitute: Did the Indian ...	Apr 18, 2012	
🟩		Mohammad Azharuddin is the onl...	Apr 18, 2012	
🟩	✓	"the first indian missile that has th...	Apr 18, 2012	
🟩		RT @cricinfo_record: It is the fifth ti...	Apr 18, 2012	
🟩		Mohammad Azharuddin is the onl...	Apr 18, 2012	
🟩		RT @hormazdsorabjee: Ertiga gra...	Apr 18, 2012	
🟩		Mohammad Azharuddin is the onl...	Apr 18, 2012	
🟩		Who's riding?@Vespa_IN We're o...	Apr 18, 2012	
🟩		RT @Wankatesh: Who's riding?@...	Apr 18, 2012	
🟩		We're on Twitter! And weâ€™re re...	Apr 18, 2012	
🟩		RT @Vespa_IN: We're on Twitter! ...	Apr 18, 2012	
🟩		#"the first indian missile that has t...	Apr 18, 2012	
🟩		RT @cricinfo_record: It is the fifth ti...	Apr 18, 2012	
🟩		RT @cricinfo_record: Mohammad ...	Apr 18, 2012	

```
<record>
author: shashj
date: 20120418063257
content: "the first Indian missile that has the capability to deliver a nuclear warhead out to any part of China" to be tested http://t.co/7v6EI0B2
language: en
retweet_of:
mentions:
tags:
</record>
```

Developed by Pacific Northwest National Laboratory's tool IN-SPIRE, this data visualization includes topic themes and a timeline of theme frequencies.

Visual analytics can also identify data that are not relevant for analysis. In one case study looking at how missile tests by India were reflected in social media, the research team inadvertently collected a large amount of data regarding

Sample Visualization of Real-Time Topic Trending in Pacific Northwest National Laboratory's Scalable Reasoning System (SRS) Related to Hydraulic Fracturing



TOP HASHTAGS	
10.7K	#Fracking
3.4K	#NATGAS
1.4K	#Energy
990	#oil
827	#shale
692	#gas
507	#News
467	#EPA

TOP MENTIONS	
2.9K	@YourAnonNews
1.3K	@NIGovCuomo
1.1K	@fractivist
740	@yokoono
481	@TXsharon
447	@EcoWatch
372	@SeanOnoLennon
319	@HuffingtonPost

TOP AUTHORS	
1.2K	RMB Group
495	marcellus protest
278	D.J. Turner
227	Mike Millard
223	frapit
219	Daniel J Sobieski
200	fractivist
152	FulbrightEnergy

TOP LANGUAGES	
39.1K	English
4.2K	Spanish
4.1K	Dutch
3.8K	Catalan
3.3K	Danish
1.9K	Norwegian
1.3K	German
1.1K	Italian

An example of data visualization for monitoring how a subject is being discussed on Twitter in real time.

cricket matches based on dual-meaning keywords in the search. Through data visualization, the team quickly identified the group of data that was cricket specific and not relevant to the missile study. Visual analytics can help an analyst to identify themes, changes, or relationships that are not apparent in text alone, or would require significantly more interaction with the data to discover.

can then be used to understand and characterize phenomena within the network.[64] Content analysis evaluating linguistic cues may also indicate the ties among people, including the sender's relationship to the receiver. Social media content may be used to determine the characteristics of an online community, such as its militancy.[66] Other work has been used to understand social media users' personalities from publicly available information in Facebook profiles, such as self-description, status updates, photos, and interests,[67] as well as linguistic cues.[68]

Forecasting

Predictive analysis seeks to use social media indicators to predict future, real-world events. Movie revenues can be predicted by the volume of chatter about a movie on

Twitter. As with any predictive capability, especially those involving human behavior, expectations about accuracy should be realistic. Validation of prediction systems is a notoriously difficult problem, as often past events do not generalize well to future ones. Forecasting based on social media–derived data may use a combination of techniques, including sentiment analysis, graph analytics, and influence analysis.[69] One could pose a query regarding the date of the next Non-Proliferation Treaty preparatory meeting and analyze how much chatter leading up to the event has taken place in previous years. Other, less cyclical events might also be predicted, such as the events leading up to a missile test. Often predictive systems report likelihoods of their forecasts to explicitly convey the level of confidence in the predictions.

MOBILIZATION FOR SOCIETAL VERIFICATION

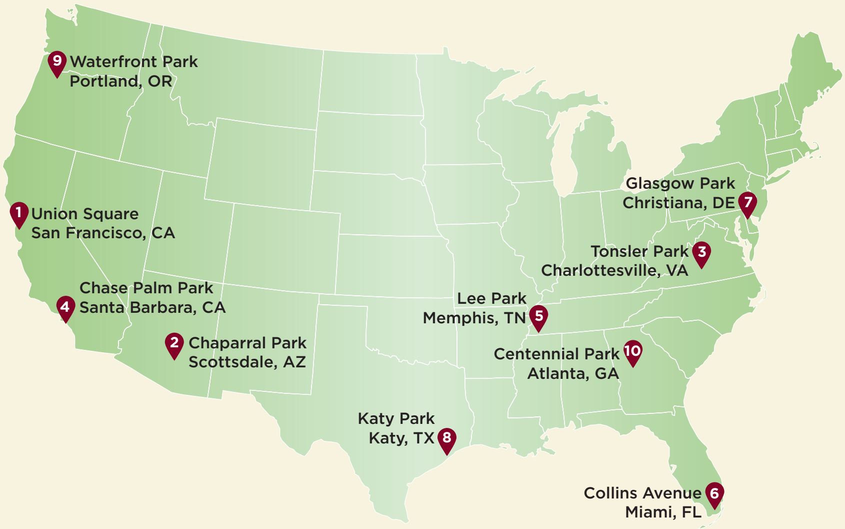
Mobilization—tasking citizens to report on the activities of their governments—was the original concept of societal verification. Now mobilization is a more nuanced, expanded concept. Beyond engaging people over communication platforms, online tools are increasingly used to mobilize individuals or groups. Mobilization for societal verification could challenge citizens to gather information regarding potential violations of treaty obligations. Digital capabilities have grown significantly around the world, especially in the use of smartphones with powerful wireless communications connectivity, built-in sensors, geolocation capabilities, unused computing capacity, and data storage. These technological advances make ubiquitous sensing very attractive as a supplement to NTM and international data collection and analysis systems. The benefits of social platforms to mobilization range from simply an efficient means of getting the message out to providing incentive structures for participation. The function of the particular platform must be matched with the mobilization objective.

While technology has made mobilization easier, there are still numerous barriers to success. Incentives can take many forms and often vary between individuals. Often, intrinsic motivation is sufficient to mobilize participants. The website Hollaback provides a platform for victims and witnesses of sexual harassment to report it. Its contributors report, in part, because they have a direct connection to the cause.[70] When causes are less personal, extrinsic rewards may be more successful. This was evident in the strategy of the team that won the Defense Advanced Research Projects Agency (DARPA) Network Challenge, in which teams had to identify, locate, and photograph 10 red balloons around the United States (see “DARPA Red Balloon Challenge”). The winning team used monetary compensation for reporting information regarding the balloons’ locations.[71]

A successful incentive strategy in societal verification may be determined by the particular region of interest. Where verification and transparency are salient concerns, programs that make reporting possible may be sufficient. Where verification and transparency are either passively or actively kept out of public conversation, extrinsic rewards may be necessary. Extrinsic rewards heighten the risk to contributors and may create

DARPA RED BALLOON CHALLENGE

The Defense Advanced Research Projects Agency (DARPA) conducted the DARPA Network Challenge social network mobilization experiment on December 4, 2009, to identify citizen mobilization strategies and demonstrate how quickly crowdsourcing could solve a challenging geolocation problem.



Locations of the 10 numbered balloons deployed as part of the DARPA Network Challenge.

Ten numbered red balloons, each more than 2 meters in diameter, were simultaneously inflated and moored in parks across the contiguous United States. All of the balloons were visible from roadways in public areas with pedestrian access.* DARPA officials were dispatched at balloon locations to verify that a balloon was an official DARPA balloon. The first person (or team) to report to DARPA the correct locations of all 10 balloons was awarded a $40,000 prize. A total of 4,367 individuals registered in the DARPA Network Challenge.** The final report concluded that at least 50 serious teams, and perhaps as many as 100 total teams, participated in the challenge, along with approximately 350,000 individuals.

* The United States has 6.5 million kilometers of roadways and all balloons were located within cities or metropolitan areas.

** Because teams often had multiple registrants per team and because DARPA did not require team affiliation to register, it is impossible to accurately extract the number of distinct teams participating.

suspicion of entrapment. Intrinsically motivated mobilization, especially when it conflicts with government interests, is likely to be spurred by social movements that create the foundation for a change in a populace's attitudes and opinions toward institutions. The success of these movements depends on a number of factors, including regional conditions and the organization of the movement itself.

Societal readiness is an important consideration. If conditions are not conducive, verification actions may be difficult or impossible. Factors that have proven crucial in other issue areas have included an active group of interested citizens, a strong cyberactivism culture, and a relatively high rate of diffusion of Internet use.[72] These qualities may not be entirely necessary, but should be considered by those planning on using new media for societal verifications.

The best approach to social mobilization may be to tap into existing interested groups and foster new networks of citizens and experts. Such networks support cooperation and solidarity, and movements build trust and develop positions naturally, without resentment and suspicion that might arise from directives passed down.[73] This approach may be particularly successful when participants are initially motivated by dissatisfaction with the actions of leadership, such as treaty non-compliance. Networks can respond quickly to a specific task, serve a purpose only as long as the purpose is needed, and do not need to rely on one leader, but can be kept to an objective through soft management.

Local adaptability is crucial, as mobilization incentives and media campaigns vary widely by culture. Effective mobilization strategies often require a combination of communication types, such as a mix of social media messages and face-to-face interactions.[74] Once social and political networks are engaged, global support and participation may follow, especially if the cause can be expressed as a problem for humanity at large, such as nuclear non-proliferation.

A challenge to mobilization, not present with observation, is the potential for competitive or countermobilization. If populations actively engage in verification monitoring, parties may try to uniquely access the information generated, disseminate or quash relevant data, and offer competing incentives to the public for participation. Another challenge is that any activity that resembles the recruitment of citizens to spy on their own (or others') governments is potentially dangerous for both the mobilizer and the mobilized. Before any country engages in such activities, legal, ethical, and moral questions will need to be answered in an open dialogue with treaty partners and the public.

6. Potential Models of Societal Verification

The value of societal verification, whether through observation or mobilization, is its flexibility in the types and amount of information it can offer to states to conduct treaty monitoring and make compliance determinations. Its role differs from intelligence gathering because it must be in the service of implementing a specific treaty or other commitment that has defined objectives and describes allowed and proscribed activity.

Societal verification could be included in national verification approaches for existing agreements without additional negotiation. Existing arms control treaties, including the New Strategic Arms Reduction Treaty (New START), allow for states to use open sources to assist their verification efforts. Societal verification techniques may be similar to using national technical means (NTM), open source intelligence, or other tools at the disposal of governments. States can immediately tailor their collection, assessment, and application of data to treaty-specific goals. States make compliance determinations, and have a lot of information available to them, but need political will, technical tools for analysis, and institutional processes in place to benefit from societal verification.

One area that might prove most useful is the public acknowledgement of the value that non-governmental expert communities can contribute. External experts have the time and flexibility to creatively approach societal verification data and can interact with one another with fewer institutional barriers in the way, including among experts with diverse competencies. If engaged, motivated, and acknowledged as valuable contributors to verification, these experts can be force multipliers. In this way, the immediate value of societal verification would be to increase accountability on the part of states for the conclusions they reach about compliance because outside experts will also be conducting analysis and reaching their own—more public—conclusions.

In the future, cooperative observation using societal verification tools may be appropriately integrated into negotiations of legal agreements. States can jointly address and agree on issues of mutual concern regarding societal verification and monitoring tools. Societal verification data does differ significantly from NTM data in that the data are a common, shared resource that would not encounter classification or other related barriers for joint examination of the information. Other factors that might prove valuable for joint discussion in the context of treaty negotiations include clearly defining societal verification for the purpose of the proposed agreement; committing to non-interference in societal verification, within the context of an agreed scope of activity; jointly developing societal verification tools and methods; defining legal protections for citizens engaged in societal verification activities; and creating a process for reporting gathered data to national authorities, ensuring that data are provided equally to all parties. States involved in such a dialogue must recognize that there is a risk of unfounded accusations. Information may be provided without relevant context and the process may be subject to manipulation. But these issues are not unique to societal verification. The broader objective is increasing engagement, increasing confidence, and creating a system that can manage the challenges.

The subsequent sections discuss four possible models for societal verification, focusing on applicable conditions, timelines, sensing versus analyzing data, available resources and technologies, important actors and their relationships, and achievable verification objectives. Table 3 offers a summary.

NATIONAL OBSERVATION

National observation refers to societal verification measures states can take that do not require mobilization of the general public or subgroups of the general public in monitored countries, nor do they require agreement among states regarding which tools will be deployed and how they will be used. In theory, such verification measures can be put to use immediately after the methodology, tools, and technologies and the infrastructure to implement them are developed.

Verification generally consists of two parts: sensing and analyzing. Sensing is the process that collects data. Analyzing is the process that studies and understands the data to draw conclusions about compliance or non-compliance in the monitored countries. For national observation, a country collects data on its own by passively watching and observing. It would mostly likely have to analyze the data itself, but it is possible that the expert community in the monitored country or other countries can be partially involved.

New media is an important catalyst for national observation. It is connected in various ways to traditional information channels, such as government-released information, media reports, academic publications, and online forums, all of which can be monitored. The challenge is to develop methods and technologies to filter and analyze large

Table 3: Four Models for the Use of Societal Verification: Characteristics and Examples

1. National Observation	**2. National Mobilization**
• Applicable in the near term • Does not require cooperation from the monitored country • Methodology, privacy considerations, and technology development are key ***Example:*** Monitoring activities of key technical experts, such as changes in publishing patterns or unusual gatherings in unexpected locations	• Applicable when connections with the general public of the monitored country can be established; does not require cooperation from the monitored country's government • Education campaigns to engage with the public of the verified country are important • Could put participating individuals at risk ***Example:*** Detecting movement of nuclear weapons transport and support vehicles or visible signs of non-compliance
3. Cooperative Observation	**4. Cooperative Mobilization**
• Applicable when treaty parties are willing to incorporate observation measures into verification regimes • Countries could face growing pressure to embrace cooperative observation in the mid-term, as new technologies empower more individuals • A joint dispute resolution mechanism could help address concerns raised in this process ***Example:*** Detecting nuclear weapons testing through routine environmental data collection	• Applicable when a significant amount of trust exists among treaty partners or in special situations when a monitored country wants to prove its innocence • Most likely feasible only for long-term scenarios • Brings about the highest level of confidence about compliance ***Example:*** Tasking citizens to monitor operation of enrichment facilities, or construction of new buildings in current nuclear complex

amounts of data in an effective and timely manner. Advanced computational algorithms need to be developed to analyze text, images, and videos in the appropriate linguistic, political, and cultural contexts. These technologies also need to be repeatedly tested in practical scenarios to improve their capability to identify reliable patterns, shifts, and indicators that can effectively distinguish useful signals from background noise.

Third-party actors such as the International Atomic Energy Agency and the Comprehensive Nuclear-Test-Ban Treaty Organization may help by participating in joint technology development. However, because these international organizations have limited legal authorities and human resources, state governments, non-governmental organizations, and independent researchers would do the bulk of the monitoring and analyzing work. National observation is most likely to be successful against violations that present patterns or send signals that the general public can pick up and share, either intentionally or accidentally. Signals that would only alert experts but appear normal or uninteresting to the general public are less likely to garner public attention.

NATIONAL MOBILIZATION

National mobilization measures are applicable when the monitored governments are unwilling to mobilize their own citizens to participate in societal verification, but those responsible for monitoring can engage the general public or subgroups within those countries in direct or indirect ways.

National observation is most likely to be successful against violations that present patterns or send signals that the general public can pick up and share, either intentionally or accidentally.

Monitored governments unwilling to mobilize their own citizens may be concerned about the potential negative effects of societal verification on domestic political stability. Officials might fear that opposition parties will abuse societal verification to fulfill their own political objectives through fabrication or exaggeration. They might also be concerned that the citizen reporting mechanism in a cooperative societal verification agreement will drive a wedge between other governments and their own. As a result, national mobilization measures are more likely in countries with mature democracies, a high degree of domestic political stability, existing trust with the monitoring entities, and a process in place to balance the needs of secrecy and openness.

As described earlier, data can be collected by encouraging the public in the monitored countries to provide information. Monitoring entities can also encourage certain subgroups within the general public, particularly experts and expert communities who may have an interest in participating in policy debate on disarmament or non-proliferation, to help analyze the data. The experts could be helpful in analyzing the data and cross-checking for errors that may result from non-native analysts' lack of understanding of local language and cultural background. These experts could contribute to more objective analysis, which is in the interests of monitoring and monitored countries. Technologies or mechanisms must be developed to facilitate communication and data sharing, not only among experts within the monitoring entities, but also between them and independent expert communities.

Engaging with and encouraging the general public in the monitored countries to provide data can be risky, as monitored governments may interpret such measures as hostile. If measures are not pursued responsibly, there is a risk of undermining implementation of the underlying treaty or agreement. The monitored governments may retaliate and become less cooperative toward existing verification agreements, complicating verification work.

One way to engage the public is to educate and raise awareness about proliferation risks and the non-proliferation obligations of their governments. Public education campaigns can focus on international nuclear non-proliferation regimes in general, but should also include specific non-proliferation and arms control agreements that involve the monitored countries. Signatory countries should widely publicize any bilateral or multilateral treaties in this issue area. Those responsible for treaty implementation, including relevant international organizations, should help educate the public about the specific non-proliferation and arms control obligations of their governments and help them understand and identify signals for violations. This would increase the public's awareness and capability to provide useful data when violations occur. Public education campaigns also can also help raise awareness among foreign citizens living and traveling in monitored countries. Social media can be useful in carrying out such campaigns. Active public engagement can increase the possibility of detecting clandestine nuclear facilities by increasing the willingness and capability of the general public to monitor and report violations. More important, broad public participation in monitoring and reporting serves as a deterrent for governments considering violating their obligations.

COOPERATIVE OBSERVATION

Cooperative observation applies to scenarios in which governments incorporate observation measures into negotiated verification regimes. Monitored countries may be willing to set up a joint dispute resolution mechanism that addresses suspicious cases collected by societal monitoring technologies. As telecommunication technologies continue to empower individuals across the world, countries may conclude that societal monitoring by others will occur whether they like it or not. Countries may find it in their interests to resolve disputes raised by societal monitoring to preserve their reputations. In cooperative observation, the monitored governments may not help with collecting data but could aid in analysis as part of an official process to resolve disputes within an arms control or non-proliferation treaty.

The technology requirement for cooperative observation is the same as that for national observation. But official dialogues and negotiations are needed to set up a mutually acceptable mechanism for resolving disputes, in which societal monitoring technologies

THE OPEN-SOURCE INTELLIGENCE MODEL

Open-source intelligence (OSINT) is the collection and analysis of publicly available information to address intelligence problems and questions. There are two approaches to using new media in the information collection and analysis process. One approach is to consider it as a new *int*, "SOCINT," to go along with human intelligence (HUMINT), signals intelligence (SIGINT), and OSINT. Another approach, however, is to consider these data as another open source and to continue to integrate it into the OSINT system.

Publicly available information is legally accessible in the public domain, either for free or by purchase. The public domain constitutes an enormous universe and, to the chagrin of many in the intelligence community, classified information often makes its way into it. Publicly available does not mean easily available, however. Although not classified, much information in the new media domain is actually owned and controlled by private companies. As the open-source universe grows in diversity and volume, "sources and methods"—a phrase most often associated with the clandestine domain—comes into play. The lines between OSINT and the other *ints* are blurring.

To incorporate publicly available information in intelligence assessments or operations, an analyst has to be an accepted partner within the relevant structures. For the U.S. intelligence community, this acceptance usually means security clearances, counterintelligence and legal acumen, and subject matter expertise. The intelligence aspect of OSINT entails following a chain of information where one finding leads to a new area of investigation. This process requires unique tradecraft. To embed collection and

would be recognized as legitimate and signatory parties would have an obligation to explain suspicion. Considering the experimental nature of societal verification, restrictive measures would need to be put in place to prevent abuse and reassure the monitored countries. Initially, joint disputes resolution measures could be primarily opportunities for consultations, and unresolved disputes may not be linked directly to legal consequences.

Achievable objectives for cooperative observation are similar to those for national observation measures. However, the official mechanism to resolve disputes arising from cooperative observation measures offer the opportunity to conduct official consultations to clarify facts and help build confidence and trust.

COOPERATIVE MOBILIZATION

Cooperative mobilization measures apply to scenarios in which the monitored countries are willing to mobilize their own citizens to participate in societal verification as analysis of new media and related data within such a structure would likely result in the sequestration of the analysis and product, and the loss of some potential value, such as creating common, unclassified pools of data and analysis that treaty parties and possibly the public could share.

OSINT professional standards do not exist today. Because OSINT is not the province of any one agency—in contrast with the other *ints*—no broad-based training and certification program exists to develop and maintain such standards. The result is an inability to assess the capabilities and needs of those who do, or propose to do, OSINT work. While individual agencies focus on skills, knowledge, and abilities specific to their respective niches, there has as yet been no effort to identify and develop what one might call general OSINT skills—those in which every individual in the intelligence community engaging in OSINT should be proficient. These standards and skills are an important frame of reference, not only for gauging the intelligence community's progress in tackling OSINT, but for setting a standard applicable to many potential partners outside the intelligence community, forming a necessary foundation for integrating societal verification goals and efforts.

OSINT's properties could support societal verification as part of its overall mission, but it would require major structural and cultural change to the current organization. The U.S. OSINT capability—due primarily to resource constraints—is not oriented to treaty verification. But deploying a robust national capability in service of international security objectives might boost interest in, and resources for, a strengthened OSINT model. Given the broad range of intelligence questions and issues to which OSINT can contribute, centralizing exploitation in one dedicated organization will almost invariably result in unrealized potential that could be partially oriented to treaty verification tasks.

part of arms control and non-proliferation treaties. This model is the longest-term scenario, and many issues must be resolved before it can be implemented.

Cooperative mobilization requires a high degree of trust between the monitoring entities and monitored countries. This requirement means that cooperative mobilization may only be applied to a very limited set of scenarios; but when there is already a highly trusting relationship, there may not be a desire to carry out strict and comprehensive verification measures. Cooperative mobilization may play a role if a country needs to prove its innocence. As countries engage with each other and gain experience, they may build that trust over time, making space for cooperative arrangements. Increasing dialogues and communication also may help reduce misunderstandings and break cultural barriers, and contribute to trust building in the long term.

If the global nuclear stockpile continues to drop, states may have a much greater incentive to set up strict verification measures to reassure each other. Under those conditions, cooperative mobilization may play a role. In such a scenario, the monitored countries would take measures to mobilize and encourage their citizens to report anomalies and violations. They would set up official channels for citizens to report and would establish procedures to help protect participants. The monitored countries would cooperate with monitoring entities to facilitate citizen monitoring, help analyze the data collected, and resolve disputes in a timely and cooperative manner. The monitored countries would have an incentive to take up these responsibilities not only because they trust the monitoring entities, but also because they see societal verification as a confidence-building measure to demonstrate good faith and to provide reassurance. Cooperative mobilization would provide the most comprehensive and reliable verification. Technologies need to be developed to facilitate this process, but with the help and cooperation of monitored countries, it would become easier to implement.

Cooperative mobilization can achieve the widest range of verification objectives. There would have to be formal and legally protected approaches for the general public and professional insiders whose participation might be characterized as whistleblowing. These measures can ensure that many nuclear arms control and non-proliferation activities that have few outside signatures could be more effectively verified.

7. Enabling and Connecting Experts in Societal Verification

The role and importance of expert groups is well established in the field of non-proliferation. Peter Haas famously coined the term *epistemic community* to refer to a group of acknowledged experts who use their expertise to influence policy;[75] such a community was crucial to developing the international practices and common understandings of nuclear arms control.[76] Substantial knowledge also resides with so-called communities of practice—people who may not be formal experts, but who have considerable experience performing in the subject area of expertise.[77] These everyday practitioners frequently know the most about best practices in a given field.[78]

Direct engagement with epistemic communities and communities of practice is an obvious way to expand and improve the information and solutions available to policymakers. However, it is not always obvious who belongs, or should belong, to these communities. Membership is often geographically dispersed and sometimes isolated by language or bureaucratic structure. Identifying the type of expertise required is difficult because of the outsized role tacit knowledge plays in the non-proliferation sphere.[79]

The rise of new-media technologies has made the task of identifying legitimate experts more difficult but expands the scope and speed of outreach. Blogs and social media outlets let amateur enthusiasts share their ideas and opinions with massive online audiences, sometimes reinforcing an image of expertise where there is none. The number of blogs and websites devoted to non-proliferation topics guarantees any manual approach to identify experts will be haphazard at best. Yet much applicable knowledge is found outside of the traditional academic and policy spheres in volunteer and technical communities—largely ad hoc groups of computer users with special expertise in a particular software application or platform. Because these groups are often temporary and task oriented, it is difficult to identify members in advance.

Beyond specific expertise, policymakers also need access to groups that overlap with the targeted communities to take advantage of the diversity of knowledge and perspective that leads to optimal solutions.[80] One expert said it was her graduate school experience in environmental science, not her current work at a nuclear laboratory, that was proving most helpful. She found an amazing similarity between the problems of inventorying nuclear weapons and determining the true population of field mice in a meadow.[81]

Traditionally, experts have been identified through a variety of cataloging methods. A person or group with subject matter expertise would examine a variety of sources and create lists of experts. Typical sources included professional journals, membership lists in professional societies, conference rosters, faculty lists, and personal networks. Online sources such as websites and blogs were eventually added to the source pool as well, but the technique of collection remained the same.

The rise of new-media technologies offers improvements to the traditional method. First, semantic web searching techniques are rapidly augmenting basic search engine technology. Although still in its infancy, the widespread use of subject matter tags and other metadata make identifying relevant documents and their authors increasingly easier. Second, social networking sites allow and even encourage experts to self-identify. Many profiles contain personal information such as hobbies or education that can give important clues as to relevant secondary expertise. Finally, there is considerable evidence that the sociological concept of homophily—that birds of a feather flock together—holds true in online as well as offline networks.[82] Consequentially, examining the online friend network of one expert will likely lead to the identification of additional similar experts.

The scale of new media offers another advantage. Experts can easily nominate other experts, who in turn can nominate others, leading to a snowball effect. Even in the absence of a nomination, the reach of networked media allows an advertisement for given expertise to circulate through large numbers of passive and active followers. On Twitter, any message interesting enough to be repeated (retweeted) by one additional user will appear in the message timelines of more than 1,000 additional people on average.[83] This message spread is especially useful in identifying interested outsiders and others who may not be experts in the subject matter, but serve as bridges between disciplines. The engaged outsider or hobbyist often serves as a catalyst for new innovation or provides the unique solution experts overlook.[84]

The availability of so much online information also allows expert searchers to use computer-assisted analytical techniques. Data scraping and mining software can automatically crawl millions of websites to compile relevant information for analysis, and some companies, such as Twitter, offer direct access to their user data through application programming interfaces (APIs). Social network analysis can identify communities with shared connections, which can be used to identify the key individuals within each community.[85] Researchers have used these techniques to identify emerging topics of interest within the scientific community[86] as well as to establish patterns of collaboration.[87] Additionally, new developments in natural language processing (NLP) are allowing programmers to generate automatic expertise profiles based on public data such as publications or online discussion groups.[88]

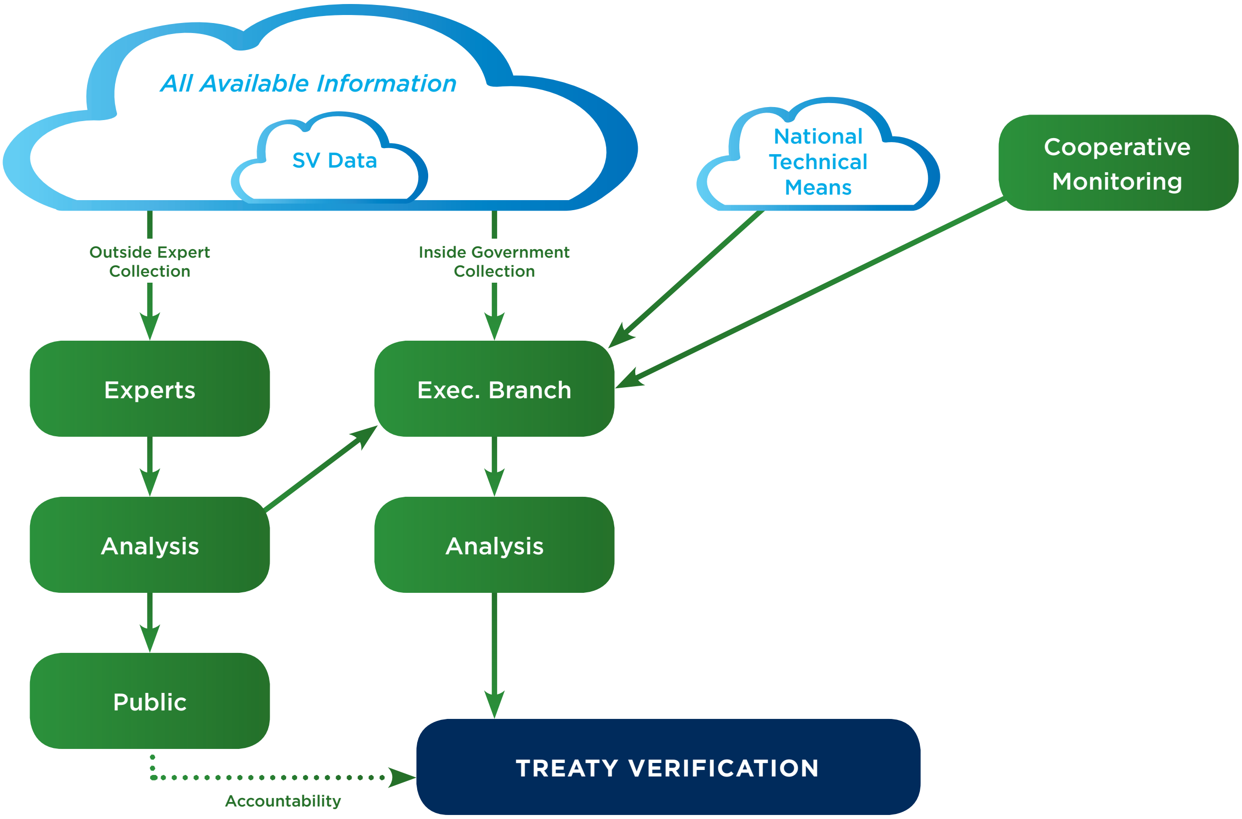
Once experts are identified, the next challenge is to encourage participation and foster collaboration. The payoff can be large, as crowdsourced group efforts have provided some of the best documented and most successful uses of social media technologies.[89] Crowdsourcing efforts such as Wikipedia or the Andromeda Project often use amateur inputs. But the majority of successful crowdsourcing efforts are the result of expert interaction.[90] The online film rental service Netflix offered a prize of $1 million to anyone who could improve their recommendation algorithm. The winner was an expert metagroup made up of smaller expert programming groups who decided to pool their efforts.[91]

Crowdsourcing is known to provide superior solutions to discrete or spontaneously produced problems, such as guessing how many marbles are contained in a jar or finding an optimum walking path.[92] It is also well suited for sustained problem solving, and difficult problems seem particularly well suited for an expert group. In a study of crowdsourced science company Innocentive, Karim Lahkhani and his team found that expert crowds solved one-third of the challenges presented to them[93]—impressive results, considering the problems had stumped the research laboratories of the world's leading scientific companies.

Incentives for expert participation in crowdsourcing or large-scale collaborative efforts differ from those typically offered to non-experts. Amateur contributions may be motivated by financial incentives and clear directions,[94] but expert participation relies on a subtle combination of factors. Love, glory, competition, the collaborative spirit, and monetary reward are all motivators for expert communities.[95] Online participation behaviors have been shown to vary according to the type of community structure,[96] the norms and commitments established for the group,[97] and psychological and social factors.[98] Researchers have yet to identify the ideal combination of incentives, but agree that incentive structures must be developed with full reference to the specific challenge and to the characteristics of the expected contributors and their affiliated communities. Because experts are engaged, this approach avoids some of the pitfalls of broader societal mobilization.

Analysis from outside government channels can hold governments accountable for the compliance conclusions they reach and can cue government inquiry into specific concerns. However, expert contribution to verification can be most effective if it is fully integrated into national monitoring efforts, adding value to monitoring and verification systems and helping use dedicated national resources more effectively and efficiently—leading to a system that works faster, cheaper, and better (see Figure 7).

Figure 7: A Model for Integrating Societal Verification (SV) in U.S. Treaty Verification



In this model, two paths connect to help the United States assess treaty compliance. On one path, the executive branch analyzes available data combined with national technical means and data from cooperative treaty monitoring (including on-site inspections). In parallel, outside experts, individually or collaboratively, analyze information and make public assessments about states' activities. This expert information would be an additional input to the official verification process and may raise additional questions or cue further examination by U.S. officials. This valuable contribution by outside analysts serves as government accountability.

8. Technical Challenges

Societal verification faces many of the same technical challenges as other big data information analytics research—mainly accessing, storing, and processing information; verification of sources and dealing with misinformation and deception; and fusing various types of data. The sheer volume of data generated through new media makes it challenging to collect, process, and analyze. New media research also faces some challenges uniquely its own. Ethical issues—related to privacy issues, concerns about unintended consequences of data disclosure, and the integrity of methods to distill the data—surround the use of social data for societal verification. This section describes some of the specific technical challenges inherent to societal verification.

IDENTIFYING THE INTERESTED POPULATION FOR SOCIETAL MOBILIZATION

Any effort at societal mobilization must first identify the population to be mobilized. This could be determined based on geographic location, occupation, demographic information, culture, special interests, or other characteristics. Communities to be mobilized might include expert communities in the particular area of interest, such as scientific organizations, or knowledgeable insiders—those who have special access to information of interest to the mobilizer. Existing interest groups may also be approached, including individuals ranging from non-expert to expert who believe that suspicious, illegal, or otherwise questionable activities are taking place and wish to report on them. Examples are environmental watchdog groups monitoring air and water quality or antinuclear groups attempting to monitor activities at government sites. The general public may be less inclined, or less technically able, to be mobilized to report on information of interest. However, some data from the general public may be useful for societal verification. Public information was effective in law enforcement for years through the television program *America's Most Wanted*.

In addition to identifying the population for mobilization, there must be a way to make the public aware of mobilization activities. The DARPA Red Balloon Challenge and the Tag Challenge (see "Games and Challenges") had websites advertising their games, providing instructions, rules, and forums for participants to upload their photos.[99] Individuals can self-identify if there is a process by which they can do so and benefit from any incentives.

GAMES AND CHALLENGES

Department of State Tag Challenge

Tag Challenge was a social gaming competition in which participants were invited to find suspects in a simulated law enforcement search in five different cities throughout North America and Europe on March 31, 2012. To win, a participant or team had be the first to successfully locate and photograph all volunteer suspects and submit verifiable photographs to the contest organizers. No team identified all five "suspects." The winning team found and photographed three targets in the shortest time.[100]

Department of State Innovation In Arms Control

In June 2013, the U.S. Department of State's Bureau of Arms Control, Verification and Compliance announced the Innovation in Arms Control Challenge. The challenge sought creative ideas from the general public to use commonly available technologies to support arms control policy efforts. The winners were:

- Allan Childers, an aerospace and defense industry consultant from Florida, who proposed a mobile application that provides a platform for users to connect and interact, as well as a rewards program for sharing information on various arms agreement regimes.
- Rudolph "Chip" Mappus, a research scientist at the Georgia Tech Research Institute working on computational neurology and brain-machine interfaces, who proposed a unique geographically based online social game for verifying treaty compliance. Experts post detailed tasks online and citizens complete tasks for rewards using photographic and human report data through smartphones and other consumer-grade hardware.[101]
- Lovely Umayam, a graduate student from the Monterey Institute of International Studies at Middlebury College, who developed Bombshelltoe, an online education platform that examines the intersection of culture and nuclear issues to facilitate better public understanding of basic nuclear and arms control–related issues.

DEFINING MOTIVATIONS FOR SOCIETAL MOBILIZATION

Societal mobilization requires some form of sustained motivation to encourage participants to spend their time collecting and providing data. Some individuals might participate out of their own goodwill, or because they want to play a part in preventing international proliferation of weapons of mass destruction. There may be stark differences, however, in engaging the public where there is general consensus about the public benefit (e.g., protecting the environment, stopping crime) and where opinions differ regarding the value of the activity to be monitored (cooperation with former adversaries, reduction in nuclear weapons). As arms control and non-proliferation are less well understood than other policy areas, the pool of available participants may be smaller and the educational process more difficult. One part of defining participants' motivations is communicating the objectives of the efforts.

In the Red Balloon Challenge and the Tag Challenge, participants were motivated by cash prizes for correctly and completely addressing a question for which there was a known answer. In non-proliferation, the solution is unlikely to be known. Cash prizes might be used as they are for criminal cases and may lead to such an overflow of information that researchers cannot process it all. On the other hand, information leading to the capture of Osama bin Laden could have earned an informant $50 million, but no one came forward for more than 10 years. The individual or group with the greatest access to important data may be the least interested in sharing it.

FINDING MEANING IN THE NOISE

The majority of data collected through societal observation will not be relevant to non-proliferation verification. Even when looking at keywords from defined signatures or information surrounding a specific event through a focused search, social media is an inherently noisy source of data. In social data monitoring for societal verification, it may be useful to look for co-occurring spikes or anomalies, either within one social platform, or across several. Sometimes there might not be anything there, as a theme or time spike might be coincidental or require disambiguation. Such validation may lose the lone voice that has a piece of uniquely relevant information, but this risk can be reduced by posing the right query.

The relevance of social data from mobilized social media communities depends on what data the community is asked to collect, how well it can be trusted, and what the question of interest is. A mobilized social media group might be asked to take Geiger counters or other radiation detectors with them everywhere they go for one week and submit digital results with global positioning system (GPS) tags. That data, provided the group has access to detectors, should be relatively easy and straightforward to collect—and, unless someone hacks or otherwise interferes with the GPS data, it may be fairly accurate and useful. It will be much more difficult to ask a mobilized social media group to identify every missile present during a national military holiday, as identification requires the group to recognize specific missile types and the differences among them. A site requesting photos of those missiles paired with locations of sightings may be more successful.

Societal mobilization methods are likely to be completed in case study formats, specific to the population being mobilized and the purpose of mobilization. The analytical methods for societal mobilization are less defined than those for observation. Analysts working with societal mobilization will be responsible for processing and analyzing datasets, but they will likely be smaller, more focused datasets than those found in societal observation.

MANAGING DATA VOLUME

While improvements in high-performance computing technologies, including those in hardware and architectures such as cloud computing, have greatly increased our ability to process data, the average analyst does not have access to the computational resources required to process and analyze the massive amounts of social data available. With hundreds of millions of tweets per day and 3,000 pictures uploaded to Flickr every minute, analysis is cumbersome. Filtering can overlook important information, yet the volumes of data make it prohibitive to go back in time for more comprehensive searches. The current state-of-the-art analytic systems can only make use of around a million tweets in a usable format for sensing applications and only around 200,000 tweets for deeper analytic applications.

Data volumes are an important issue for social media research because the analytical tools are hosted on the Internet, which limits the analytics' scalability. Building an enterprise solution is ideal, but given the amounts of data, the approach is very cost prohibitive. For now, web applications are the state of the art.

FUSION OF MULTIPLE PLATFORMS

Despite the wide availability of social data, little has been done in fusing multiple data types. Current social media analytic solutions can analyze microblogs, social networking information, and photo data, but they are rarely incorporated into a single analytic environment. Currently, only a small portion of social data is geotagged. With geotagging, social data could be analyzed within a geographic context. Some text, while not geotagged, refers to geographic location within content. Some vendors can attempt to geo-bound social data through an Internet protocol (IP) address. Limiting one's data collection to only social data with geotags would constrain results. When social data are independent from geographic information, it may be difficult to determine whether the social data are coming from the community of interest.

DATA OPENNESS

Although data availability is improving, much of the most useful data are in restrictive formats or simply not publicly accessible. The U.S. government is attempting to address this issue with efforts such as the Digital Government Strategy,[102] but progress has been slow. Standardized application programming interfaces to access public domain information held by governments and international organizations are still needed. Until then, public domain data, such as trade statistics or radiological source registries, will not be able to provide the same insights that big-data analytical techniques currently in use in the private sector offer.

TOOLS TO ANALYZE DATASETS BEYOND TWITTER

Most open and available state-of-the-art social data analytical tools are Twitter-centric. Facebook data is starting to be analyzed as well, but these analyses need to be much more platform agnostic. The volume and format of data generated by Twitter users lends itself to use by developers of technical tools. Most analytical tools for social media data beyond Twitter and Facebook are still in pilot deployment phases. As a generally English speaking–centric platform, Twitter's breadth for societal verification is limited, except when users are specifically targeting messages to the United States. As such, analytic tools that go beyond Twitter's dataset are needed to process potentially relevant information.

CHALLENGES WITH LANGUAGE

Disambiguation

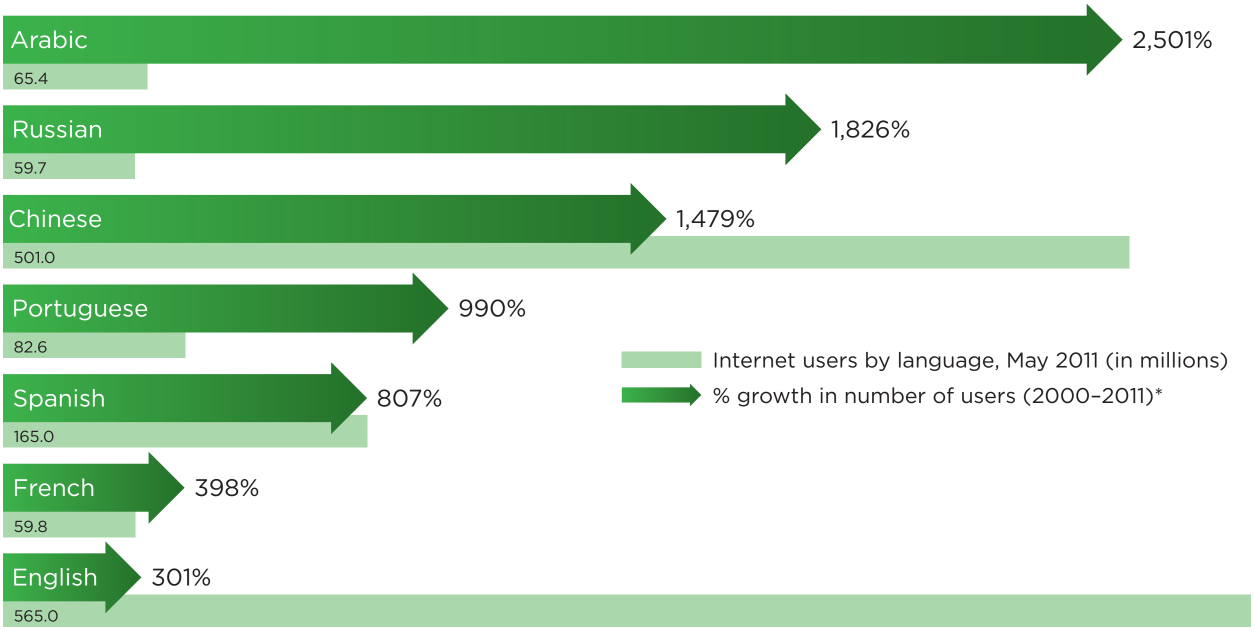
Disambiguation refers to determining the difference in meaning between two words that are the same or essentially the same. In the social media context, this becomes relevant when social data are searched by keyword or used in an analytical tool to determine themes. Presence of a keyword with the wrong meaning can lead to incorrect results.

If an analyst looking for information regarding U.S. missiles employs the word "minuteman"—the name of a type of missile—some search results will lead to Revolutionary War history and reenactments. It is useful to know the various ways in which search terms can be used before purchasing data. Analytical tools can also help filter out unwanted uses of search terms by identifying themes within a keyword search that are not relevant to non-proliferation or arms control (such as Revolutionary War reenactments).

Foreign Languages

While one can search in and filter foreign languages, the majority of language processing capabilities are specific to English. The usefulness of social media as a resource is limited until major progress can be made in this domain. Just as social media analytics need to diversify to platforms beyond Twitter, non-English-language social media data are likely to be crucial for societal verification through social data monitoring. Enhanced translation capabilities are needed that will not only recognize words or sentences, but pick up on language nuances, such as idioms and sarcasm. Some work is being conducted in non-English-language social media. That research needs to continue to grow until capabilities are sufficient for languages in all areas of potential societal verification interest. This capability will prove important, as the growth of non-English-speaking users online has been dramatic and is projected to rise quickly (see Figure 8). In 2006, more than 80 percent of Internet content was in English; by 2016, more than 80 percent will be in a language other than English.[103] One wrinkle in the non-English-language

Figure 8: Language Growth on the Internet, 2000–2011



*Numbers have been rounded to the nearest 1%.

Source: Internet World Stats, http://www.internetworldstats.com/stats7.htm.

As non-English Internet traffic grows, developing tools to collect and analyze data in other languages will be even more important.

challenge is that posed by slang or usage that is particular to niche communities or specific platforms.

Illiteracy

Illiteracy has been identified as an access issue for social media, as illiterate populations are much less likely to contribute to social media than their literate neighbors, friends, or fellow citizens. However, new innovative techniques incorporate illiterate populations into social media communities. Researchers in Pakistan are working with a voice game that helps illiterate people understand a voice messaging system to scroll through job listings.[104] In a different study, Sugatra Mitra installed computer terminals in rural India with content related to biotechnology of DNA replication in English. Children who were not English speakers and who had not previously been exposed to computers could interact with the information and learn about the topic.[105]

Illiteracy, however, is not such a hindrance to analyzing society-produced information, as smartphones with video and photography capability are rapidly spreading even in regions widely considered to be technologically lacking. Nigeria reports 73 percent of its population owning mobile phones, with the ability to use social networking platforms cited as a likely driver.[106] The challenge that non-text content produces is the ability to create semantic meaning out of pictures and video, usually requiring even greater processing power and algorithmic sophistication (i.e., image processing, image recognition).

EVASION AND COUNTERMEASURES

Regarding satellite imagery, just as telegraphy led to the use of codes and the development of code breaking, the ubiquity of satellite imagery has increased camouflage concealment and deception efforts against overhead detection, identification, and assessment. In 2006, a Chinese military journal article asserted that Google Earth "has broken the monopoly position of traditional line-drawn maps and ushered in a new era of electronic maps [but] has also brought a certain amount of hidden security-related dangers that pose threats to every country and region." The author recommended the adoption of "various methods and measures and do all we can to get around the problems brought about by Google Earth and minimize the impact it has on national security," and stressed "the importance of anti-reconnaissance against satellites, properly camouflaging and protecting important secret facilities, and understanding a satellite's shooting intervals, which could be used for conducting major military activities."[107] India and Norway have also reportedly implemented such evasions and countermeasures by developing ways of "hiding defense installations from satellites, and would find other ways such as concealing buildings underground and in mountain installations."[108] Such efforts are not surprising, as they have been extensively employed since the dawn of aerial reconnaissance and are rarely successful.[109]

9. Policy Challenges

Societal verification shares some policy challenges with other verification and monitoring approaches but also has some unique concerns. Issues of privacy, data confidentiality, and legal oversight must be managed. Societal norms influence whether and how societal verification can be used in different countries. These issues are constantly evolving and pertinent standards and policies may not be created or accepted in the near future.

Societal verification limitations and concerns vary depending on the type of societal verification. Majority legal opinion in the United States currently holds that once data are posted to a social media site, they are public information. This opinion is not universal and the standard is changing. Public opinion, however, is confused about the nature of the protection of a person's online information. Many people using social media know that the information they are presenting is public and may be viewed, copied, used, analyzed, or recorded by others. But not all information that ends up on social media has been made public intentionally. Even if information is considered public, a number of legal and ethical challenges remain regarding the use of social data. Because social media analytics is a relatively new field, researchers point out that its progress is outpacing the consideration of ethical issues.[110] The business and marketing communities have conducted the largest studies on the ethics of social media research, as they tend to be the largest users of the data source. Journalists have also had to grapple with these issues.[111]

Most of the ethical issues surrounding the use of social data for societal verification reflect general concerns broadly applicable to the use of social data for any purpose. They largely center on privacy issues, but there are also concerns about the unintended consequences of data disclosure and the integrity and impartiality of the methods used to cull the raw data stream and establish data veracity. Many of these issues have been gathered from marketing research—the primary users of social media analytics—

and applied to arms control and non-proliferation problems. According to the European Society for Opinion and Marketing Research (ESOMAR), which has published guidelines on use of social media for market, social, and opinion research,[112] online research, including social media, should follow the same governance as information from face-to-face, mail, or telephone research. The Council of American Survey Research Organizations also provides social media research guidelines.[113] Although both sets of guidelines are targeted for market and opinion research, principles regarding privacy, doing no harm, and protection of the industry are equally valid considerations for social data research. Governance of Internet platforms and regulations regarding data are, fundamentally, nationally based. There is currently no consistent international rulemaking that applies globally.

Resolving legal issues will ultimately depend upon the country or countries in which the collection, storage, and analysis are being done; the platform from which the information was collected; and potentially, the host country of that platform. Privacy concerns in Europe differ from those in the United States. Furthermore, the provenance of the data collected may determine the legality of a collection: The U.S. intelligence community is generally prohibited from collecting within the United States or against U.S. persons. However, some cross-cutting concerns will be relevant across countries and platforms. The following sections offer an overview of the legal and ethical issues to consider for societal observation and mobilization research.

DATA COLLECTION AND USE

The collection and use of social data is laid out by each social media platform's terms of service (TOS) or terms of use (TOU). These can vary by platform and country. Many TOS have intellectual property rights clauses that explicitly forbid the unauthorized copying of material. Many go further to bar all forms of social media data collection. Subject to fair-use exceptions in certain countries, such TOS could prevent researchers from copying material to their computers for further analysis and forbid any sale of that information to clients without permission. Some TOS also dictate the capacity under which individuals can collect information from the site. Some social media platforms have rules against misrepresenting one's own identity for the purposes of data collection. In addition, there are legal issues regarding who can use the data and how. Different laws or rules may apply to different organizations.[114]

If data from social media are to be used in the context of a formal cooperative verification regime, it is reasonable to expect that all terms of service and use will need to be met. Furthermore, its collection will likely have to be legally and contractually authorized, not only in the country where it was collected, but also before an international body or court.

COLLECTION CONCERNS SPECIFIC TO MOBILIZATION

Some countries may welcome the opportunity to challenge their own citizens to help demonstrate compliance with an arms control treaty. Others may not. Some countries may view encouraging private citizens to participate in arms control or non-proliferation verification activities as espionage, even if embedded into a formally recognized and mutually beneficial cooperative transparency regime. Participation in schemes where individuals report on their own country, or a country they are visiting, could put individuals at risk of jail or other persecution. An analyst mobilizing a population to collect data that will be used for arms control or non-proliferation compliance verification, especially through deceptive or clandestine means, could be viewed as enabling entrapment, or espionage. (For one specific case study, see "Using Social Media in China for Societal Verification")

Even in the United States, prevailing practices may contribute to such perceptions. The tasking of information collection on foreign activities has generally been treated as an intelligence community equity. However, an intelligence community lead in contacting or encouraging foreign citizens to participate in verification activities might well reinforce the perception in some quarters that participation in societal verification constitutes espionage. Complicating matters further, intelligence community authorities prohibit collection on U.S. persons, but in the interconnected world of social media, ubiquitous sensing, and other modern forms of societal verification, it might prove extraordinarily difficult to disentangle information generated by U.S. persons and entities from that generated by foreign persons and entities. This will probably necessitate the creation of an entirely new national and international institutional framework—that may include but should not be led by the intelligence community—to task, manage, oversee, and regulate those aspects of societal mobilization that some countries may potentially treat as espionage. A great deal of care and expertise would need to be invested in creating such an institutional infrastructure to ensure transparency and international legitimacy.[115]

DISCLOSURE OF INFORMATION

Depending on the information being collected or analyzed, disclosure of information could put individuals or groups at risk for their personal safety or cause serious operational security concerns for facilities. Two examples of information disclosure have been widely publicized. The first was the development of Facebook's Beacon software, which connected users' online consumer activities with participating websites—such as making a purchase, signing up for a service, or adding an item to a wish list—to their Facebook account to notify their friends of the activity.[116] When the Beacon software broadcast information about users' video rentals to their Facebook friends, concerns

USING SOCIAL MEDIA IN CHINA FOR SOCIETAL VERIFICATION

China is a complex case for the application of societal verification. Its political leadership has asserted that the best way to build confidence and trust between states is to start from the top political level. From the Chinese cultural perspective, only after political trust at this level is built is it possible to cooperate at lower operational levels. The implication is that Chinese political leaders are usually skeptical about the efficacy of efforts that seek to build trust from the bottom. Therefore, the idea of societal verification may be challenging to general Chinese approaches.

Second, as most China observers have pointed out, China's decisionmakers pay close attention to domestic stability. Any effort—particularly those by outside players trying to mobilize the general public and possibly encouraging people to turn against their government—is a serious concern, as the Chinese domestic political landscape is becoming increasingly divided. Pro-democracy groups frequently challenge the legitimacy of the government and the Communist Party. In numerous cases, dissidents and opposition groups fabricated or exaggerated scandals to undermine the government's reputation and to instigate public unrest. The effect of such activities is significantly amplified through the use of social media and other information sharing technologies. Against this background, it is unlikely that Chinese decisionmakers would welcome the use of new media to mobilize their citizens to help verify their arms control obligations.

Nevertheless, societal verification could still be useful in China. There have already been both positive and negative examples in which social media was used to help study China's practices regarding nuclear arms control and non-proliferation. The study that concluded China may have as many as 3,000 nuclear weapons reveals the danger of studying Chinese social media without having someone with the analytical skills and cultural knowledge to cross-check the analysis.[117] There are also successful cases in which new and reliable information about China's ballistic missile vehicles was revealed by studying Chinese social media postings.

Efforts to apply societal verification in China need to pay special attention to the need to develop computational technologies and analytical methods that can pick up important signals from an extremely high level of background noise and verify their validity. As China has more than 500 million people online, the quantity of data produced is enormous. The technology must be able to handle not only this huge amount of data, but also to analyze the data in the context of local language, culture, and other complex social conditions.

Expert communities in China are less developed and connected than those in some other countries. Mobilizing the Chinese public may be unrealistic and may actually undermine the bilateral state-to-state relationship by creating suspicions between the governments. However, many Chinese experts may be willing to be engaged and get involved. Chinese experts have shown interest in participating in global policy debates regarding important nuclear arms control and non-proliferation issues, particularly when they are related to China. They can cross-check and analyze data collected by societal verification methods, helping to minimize cultural or linguistic misunderstandings.

arose that this might inadvertently disclose a user's sexual preferences or other information the user was not intentionally disclosing to his or her social media connections.[118]

The other common example is the retailer Target's use of predictive analytics to forecast which customers were pregnant. New parents, according to the statistician behind the analytics, "are a retailer's holy grail"[119] because they tend to shop for convenience, buying not only diapers at Target, but also groceries or cleaning supplies. Target analyzed purchasing patterns of customers and directed specific marketing toward individuals who were likely pregnant, intending to gain customer loyalty before the birth of the child. An outraged father whose daughter was receiving ads from Target for baby products later found out that his daughter was indeed pregnant.[120]

The potential ethical issues surrounding inappropriate disclosure of information are not always obvious. This may be compounded when handling big data sets such as those found in social data research, in which "the potential damage of multiple individually benign pieces of information being combined to infer, or a big dataset being analyzed to reveal, sensitive information (or information which may later be considered sensitive) is much harder to foresee."[121]

PRIVACY AND PERSONAL DATA

The dynamics related to adopting transformative information and communication technologies are discussed above. Parallel to the ebb and flow of these technologies, privacy concerns have waxed and waned, as has the associated governance framework to address those concerns. This process has been a function of place and time. Google Street View has touched a raw nerve and is prohibited or severely restricted in parts of Europe, such as Germany and Switzerland, while it has been widely accepted in the United States. Police surveillance cameras are controversial in parts of the United States, but have been largely accepted in parts of Britain. Expectations of privacy in phone conversations in the United States have changed: As party lines and human operators vanished, there was an increasing expectation that both the content and metadata associated with phone conversations would be private. In some ways, the second half of the 20th century in Western Europe and North America was a golden age of privacy and anonymity, as people moved from small towns and villages, where everyone knew everyone else, to the relative anonymity of urban life, and automation reduced direct human involvement in communications and record keeping. The recent trend toward globalization and interconnectedness, however, is edging life back toward a more intrusive norm. It would be very timely to conduct extensive research to understand past ebbs and flows of privacy concerns and, very significantly, the legal and institutional framework created to address evolving norms (see Appendix).

New-media research must comply with national and international data privacy legislation and relevant requirements for notice, consent, accuracy, security, and access when personally identifiable data are collected and stored.[122] Simply assuming mirror compliance with U.S. law—when applied to the data privacy rules of another country—can lead to problems. These issues touch on areas of access rights, proprietary information, and the respective roles of private corporations and governments. The Privacy Act of 1974 as amended governs the collection, maintenance, use, and disclosure of U.S. persons' personal information—such as name, address, education, or affiliations—by U.S. government agencies and their contractors. Rules governing the application of Privacy Act mandates to social media vary among U.S. agencies, depending on the authorities involved[123] and to some extent also on different interpretations of the rules by legal counsel in various departments and agencies.

There are also legal issues specific to the international transfer of personal data. The European Union prohibits the transfer of personal data to non-European Union countries that do not meet its standard for privacy protection. The U.S. Department of Commerce, in consultation with the European Commission, developed a safe harbor program that provides a framework for U.S. companies to satisfy this requirement.[124] A reciprocal concern is whether the country to which the data is transferred from the United States offers a level of protection in accordance with U.S. law.

New-media research must comply with national and international data privacy legislation and relevant requirements for notice, consent, accuracy, security, and access when personally identifiable data are collected and stored.

Online services make it possible in many cases to identify a poster from his or her username or comments and to link that individual or entity to many other aspects of personally identifiable data, including an address, phone number, likely income, and demographic data. Given this, data cannot always be made completely anonymous by removing the username or the linked uniform resource locator (URL) from the comment. Therefore, if researchers wish to quote publicly made comments in reports or to pass these on to people not bound by the International Chamber of Commerce/European Society for Opinion and Market Research (ICC/ESOMAR) Code—or a contract linked to it—they must first check whether the user's identity can be easily discovered using online search services. According to the ICC/ESOMAR Code, researchers must make reasonable efforts to either seek permission from an easily identified user before quoting them, or mask the comment to such an extent that the identity of the user cannot be obtained.

In considering privacy concerns, it is important to keep in mind that even the use of supposedly anonymous data may prove to be problematic. *The New Yorker* magazine has unveiled an anonymous inbox to allow whistleblowers to safely submit information.[125] Others maintain that it will prove to be exceedingly difficult to truly make posts anonymous.[126]

A CAUTIONARY TALE: DARPA'S INNOVATION AWARENESS OFFICE AND THE POLICY ANALYSIS MARKET

Government initiatives that do not adequately and transparently address the public's privacy concerns can trigger a serious backlash and create or add to a perception of excessive government surveillance.

One cautionary tale from the past comes from DARPA's Innovation Awareness Office (IAO) of the early 2000s.[127] The office supported a project called Total Information Awareness to apply surveillance and data mining techniques to detect and track security threats posed by terrorists and terror groups. The project created large databases containing personal information and then mined the data to look for signatures associated with suspicious activities. When the program became public, a furor erupted and Congress closed down the office. Another controversial IAO project was a futures market to predict political instability and other potential threats. The program may have had some value as an early attempt to explore the utility of crowdsourcing to answer security questions, but the terrible optics associated with the program became a problem. It was perceived to be an attempt to solicit bets on future terrorist attacks and was consequently found to be in extremely bad taste. The public's expectations of privacy and decorum need to be understood in designing public programs even if they intend to serve important policy goals.

PERCEPTION PRINCIPLE

The perception principle in social media analytics is a sanity check, because pure motives combined with the best of intentions do not necessarily result in ethical or moral research. To ensure compliance with the perception principle, one might ask, hypothetically, how the American Civil Liberties Union or *The Washington Post* would run with a story about a verification project, and how readers might respond.

TRUSTING THE DATA

In the process of data vetting and authentication, there is reason for optimism that deception and manipulation of social data are readily detectible, unless they are extremely sophisticated. A tradecraft has already developed in the open and classified sectors for dealing with bias when assessing information. Further tradecraft is developing in vetting crowdsourced data collection to defeat attempts at deception and manipulation. Wikipedia uses trusted editors to provide quality control and prevent the hijacking of entries. The Amazon Turk crowdsourcing service includes a feedback loop, so that the inputs from elite solvers (based on past performance) cost extra. Moderator intervention is an important ingredient in the use of public data, and the moderators have a favored status.* The associated legal and ethical issues center on the need for checks and balances to maintain the integrity and credibility of the privileged and trusted moderator community, while leaving it with enough discretionary power to be effective. In societal verification, the state edits the data; thus governments should study lessons learned from the private sector in how to vet editors of online data amalgamations, including unintentional presentation of misinformation.

HUMAN SUBJECTS

Generally speaking, observational or analytical research using social media data obtained from publicly available sources—meaning that the sources are available on the open Internet and do not require passwords to access—is not considered human subjects research, as long as analysts are not interacting (i.e., communicating) or intervening with the social media users and are not deliberately accessing identifiable private information (as may be the case in mobilization activities). However, there is a risk of crossing legal or ethical lines if it is possible, through the technical design of the project, to access identifiable private information in some manner. This encroachment might include building an unintentional mosaic of a person or gathering metadata of some type.

PROTECTION OF THE REPUTATION OF INDUSTRY

ESOMAR has identified "protection of the reputation of industry" as another important consideration for restricting social media research.[128] ESOMAR uses the term to refer to the marketing and opinion research industry. The same could be applied to the non-proliferation community. Along with the public perception principle described above, any research on social media analytics for the non-proliferation and arms control verification community should maintain the scientific and professional integrity of the organizations involved.

* For example, these moderators are frequently empowered as gatekeepers to ban users, restrict access to an activity, or enforce rules regarding the sourcing of submitted material. For a recent example of a controversial actions by Wikipedia editors aggressively acting as gatekeepers, see A. Sullivan, "Wikipedia's Blog Problem," The Dish, May 16, 2013, accessed April 1, 2014, dish.andrewsullivan.com/2013/05/16/wikipedias-blog-problem/.

EFFECT ON CONFIDENCE SPECIFIC TO MOBILIZATION

Mobilization could make societal verification into a formal compliance tool, possibly undermining voluntary confidence-building measures. This possiblity raises questions about what the move toward verifying or checking a declaration, rather than showing others for the purpose of bona fides, means for arms control and non-proliferation, as well as what the normative implications of mobilization are for a world without nuclear weapons.

With the power afforded by new technologies come many potential downsides and liabilities, including the use of these tools for counterproductive purposes by governments or other opposition parties and the risk to information providers. These considerations should be weighed when considering any societal verification program. A subtle, but potentially significant obstacle to using social media platforms for societal verification is that the tools themselves do not really create motivation, but often just augment the perceived size and power of the movement. Online participation creates the impression that an individual is involved, without requiring any real action on his part, commonly referred to as "slacktivism."

With the power afforded by new technologies come many potential downsides and liabilities. These considerations should be weighed when considering any societal verification program.

Using social media platforms to mobilize people or requiring that their participation be enabled through these types of technology risks reducing political responsibility. By merely signing up, people may feel politically involved without doing anything.[129] The use of social media may reduce mobilization; further, repressive governments may also use technological tools to suppress dissent, insert misinformation, and collect information intelligence for nefarious purposes.[130]

Other concerns about societal verification include the risk of false positives, weak motivation to put oneself at risk, and lack of information control. Relying on crowd intelligence for attribution or identification will likely lead to many more false positives, as demonstrated in the Boston Marathon bombing, when citizen reporters incorrectly identified several suspects.[131] These missteps may have severe consequences, given the propensity for vigilante justice. The weak ties that form the basis of social media also may not provide the necessary bonds that people require to put themselves at risk, such as providing information that may cause negative government scrutiny.[132] Providing information to online sources forces individuals to relinquish control of that information, where they no longer determine its dissemination and content, regardless of the claims of the communication platform.

TREASON AND ESPIONAGE

Verification would be enhanced if citizens of each state party to a treaty recognized an obligation to report sensitive national security matters that challenge their own nation's compliance to treaty partners or international organizations. However, most countries currently would consider such reporting to be espionage or treason. The U.S. Department of Defense defines espionage as "the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation."[133] Espionage is a violation of 18 United States Code, Sections 792-798 and Article 106 of the Uniform Code of Military Justice.18 USC Sec. 793 reads, in part:

> (d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document … or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated … the same to any person not entitled to receive it … shall be fined under this title or imprisoned not more than ten years, or both.

Information related to the possible violation of provisions in an arms control or disarmament treaty or agreement would necessarily relate to national defense. Reporting such information to another country or an international body could be expected to injure the target country or its reputation. Citizen reporting flies in the face of existing norms of behavior in the United States and in most modern nation–states.

The U.S. standard for treason is relatively constrained. According to Section 3 of Article III of the U.S. Constitution, "Treason against the United States, shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort. No Person shall be convicted of Treason unless on the Testimony of two Witnesses to the same overt Act, or on Confession in open Court." Other countries are less restrictive in their definition of treason. Under Russia's treason law, enacted in November 2012, the definition of treason includes "providing financial, technical, advisory or other assistance to a foreign state or international organization … directed at harming Russia's security." In reporting the new law, *Rossiyskaya Gazeta* stated in a commentary on its website, "citizens recruited by international organisations acting against the country's interests will also be considered traitors."[134]

According to Chinese law, state secrets are defined as "matters that have a vital bearing on state security and national interests and, as specified by legal procedure, are entrusted to a limited number of people for a given period of time."[135] State secrets include secrets concerning major policy decisions on state affairs; secrets in the building of national defense and in the activities of the armed forces; secrets in diplomatic activities and in activities related to foreign countries, as well as secrets to be maintained as commitments to foreign countries; secrets in national economic and social development; secrets concerning science and technology; secrets concerning activities for safeguarding state security and the investigation of criminal offences; and other matters that are classified as state secrets by the state secret-guarding department. With regard to the general public, China's criminal law has a chapter on "crimes of endangering the state security" which generally refer to "activities deliberately taken to undermine the national interests, security, or survival of the People's Republic of China."[136] Article 110 of China's criminal law defines an act of espionage as, first, joining an espionage organization or accepting a mission assigned by the organization or its agent, or second, directing the enemy to any bombing or shelling target. These legal definitions of treason and espionage are very broad and general. The lack of specifics implies that judgment on an act of treason or espionage is very much up to interpretation by those in the judicial system.

Article VII of the Chemical Weapons Convention (CWC) requires each state party to enact penal legislation to prohibit its citizens from undertaking activities prohibited to a state party. Similarly, international agreements could require states parties to pass laws legalizing, protecting, and incentivizing citizen reporting. However, as with existing whistleblower laws, many potential participants will remain skeptical of such protections. Citizens who report on their own country can be expected to encounter strong negative reactions from their government and fellow citizens. Providing asylum or an international witness protection program for citizen reporters and their families would likely be needed, but extremely difficult to implement. The very need for such programs points to the existing strong disincentive for citizen participation.

Overcoming existing beliefs regarding loyalty and treason, which are ingrained in a significant portion of almost every country's citizenry, presents a strong impediment to constructing an effective societal verification regime. In less democratic countries, where individual rights may not be highly respected, fear of reprisal rather than a heightened sense of loyalty may be the greatest impediment to establishing societal verification. The issue of privacy as an ethical question pales in comparison to fears of reprisals or law enforcement that may result when anonymity is not possible. Methods of dealing with issues raised by providing anonymity should be explored.

PROTECTIONS FOR PARTICIPANTS

Institutional frameworks need to include legal protections for those that participate in traditional and new forms of societal verification. Extending such protections on an international scale poses substantial challenges. A treaty or convention might define an individual's responsibility to report on violations and the legal protections afforded those who engage in such reporting. Such provisions would then need to be implemented nationally by treaty signatories. The idea of a treaty requiring countries to pass and enforce enabling legislation governing the behavior of its own nationals is not without precedent. The CWC requires signatories to pass laws forbidding private entities from manufacturing and possessing chemical weapons. However, the whistleblower protection laws that backers of the model Nuclear Weapons Convention envision would need to explicitly exclude protections for those that disclose classified information. Governments have a legitimate interest in keeping some secrets when dealing with national security or military issues, and an attempt to modify the international order in a way that undercuts that interest will fail. Viable societal verification models will have to be consistent with existing rules and procedures regarding individuals that possess or have possessed security clearances related to the release of classified material.

There would be practical challenges associated with implementing exclusions for clearance holders. One problem can come from the unintended consequences of codifying such exclusions. In the United States, think tanks and non-governmental organizations (NGOs) are frequently staffed by knowledgeable people, many of whom hold or once held U.S. security clearances, and any new societal verification paradigm should do no harm to these existing activities. A carelessly designed exclusion of current and former security clearance holders from the business of societal verification might have an unintended chilling effect on the participation of think tanks and other NGOs. A second challenge involves the question of who does or does not hold a security clearance. These are clearly defined categories in the United States and most Western countries, but that is not universally the case. For an exclusion of people with security clearances to work, the concept of security clearances would need to be internationally codified and standardized, a difficult endeavor with an uncertain outcome.

PUBLIC AND PRIVATE OWNERSHIP OF DATA AND ACCESS

The rise of social media platforms has led to concern over privacy and how corporations can and should use the data consumers provide. Despite the impression given by recent European court cases and op-ed pages[137] the privacy policies of the major social media companies are unequivocal. On its support page, Google states, “to put it simply, Google does not own your data.”[138] Facebook is a bit more nuanced, stating that “while you are allowing us to use the information we receive about you, you always own all of your information.” The company also claims it makes data it shares with companies outside of Facebook anonymous.[139] Twitter’s working assumption is that it is a public platform and “most of the information you provide us is information you are asking us to make public.” Accordingly, Twitter says that public information is “immediately delivered via [Simple Message Service] and our [Application Programming Interfaces] to a wide range of users and services.”[140]

It seems clear from the privacy statements that individual users own their data. It ought to be equally clear that individual data are not worth much. The business models of all social media corporations rely on the ability to repackage the individual data, perhaps augmented by some degree of analysis, and resell it to third parties, which is likely to be the case regardless of the corporation or the country in which it is based.[141] In this context, the value of a corporation does not lie in its ownership of data, but in its role as data gatekeeper. As any attempt to combine social media and societal verification relies on unfettered access to data, the crucial role of the gatekeeper is obvious.

In August 2012, Twitter ushered in a series of changes to its application programming interfaces (APIs), the rulebook that defines how third-party software developers can access Twitter's store of user posts (tweets) and personal information. Most developers took the changes in stride, and the changes generated little attention outside the programming world. But some developers saw the situation differently. One summed up the power of the gatekeeper this way:

> They have a big kill switch—anyone at Twitter can kill me in a second, they can turn off any of my applications any time they want. They can kill all my apps and shut off all my paying clients, and they've done that. We're all terrified of them—we won't say a word.[142]

Researchers and non-profit users have also been disappointed in the change. In a discussion forum, a lead member of the development team for a free analysis package popular with academic researchers said the changes render his product "useless for all but the smallest networks."[143]

Search giant Google is equally powerful, as its decision to cancel several services demonstrates.[144] In addition to closing down its popular Google Reader service, the company is also discontinuing programming support for its shopping search tool. This has a major effect on providers of product information and the retailers who depend on them.[145] There are no free alternative providers of data, and small retailers will now be at a competitive disadvantage to larger companies that can afford to invest in private price intelligence services.

In short, there is no such thing as public data with respect to social media, only publicly available data. Social media companies make the data available at their discretion and are free to change the terms of the arrangement whenever and however they see fit. This control may be for commercial motive or to conform with the laws and practices of a country where the provider operates.[146] The benefits of publicly available data are numerous, but the limitations of ownership and access will remain a factor as long as private gatekeepers control distribution. Therefore, platforms or programs built to utilize this type of data, such as societal verification, should be cognizant that reliance on third-party data is tenuous at best.

PROTECTING ANONYMITY

To overcome the inherent risk to information providers, methods of keeping citizen reporters anonymous should be carefully explored. The problem is complicated by the degree to which data supplied can be directly attributable to an individual. It may be difficult to obscure sensor data tied to geographic coordinates originating from individuals' cell phones while retaining the facility to conduct meaningful data interpretation and authentication for data integrity. To ensure safety for verification reporting, new approaches to assuring anonymity may be required, such as information clearinghouses, wherein a neutral moderator performs data cleansing for any personally identifiable information. These approaches, much like any software, should be extremely well vetted.

There is no such thing as public data with respect to social media, only publicly available data. Social media companies make the data available at their discretion.

Platforms that provide instrumented anonymity must be carefully chosen, however. The program Haystack was created as a tool to circumvent censorship in Iran during the 2009 election protests.[147] Although praised by the U.S. government and granted an export license, the program still allowed user identification.[148] Other programs hide a user's identity, but governments that closely monitor the Internet can detect that these programs are being run and then work to disable the communication.

With the global increase of social media and the spread of new ideas and information, a so-called conservative dilemma has emerged, as a gap grows between government reports and that of the general populace. Overt censorship or outright shutdowns of the Internet, however, put the government at risk of alienating pro-government parties or harming the economy. One commentator contends that, rather than trying to "weaponize social media," the United States should concentrate on promoting free speech on a global scale. This effort would allow movements to begin organically, though at the potentially very high cost of time.[149]

Despite the challenges, the potential use of social media for societal verification should not be dismissed. Whether or not governments design approaches for using socially derived data, the information provides opportunities for others to access and take advantage of this valuable and sensitive information source. Advocacy groups have reported much success in using these tools to promote civic engagement and collective action,[150] including increased exposure, speed and ease of communication, promotion of organizational growth, lowered cost, and ability to reach new populations.

10. Recommendations

Working Group participants identified areas of critical need to advance the concept of societal verification for nuclear threat reduction. These recommendations include actions for government officials and policymakers, technical specialists inside and outside government, and other diverse expert communities, which will move societal verification from promise to practice.

Governments need to build a foundation for societal verification within the current arms control policy leadership. They should develop policies, diplomatic guidance, and bureaucratic structures to evaluate and integrate societal verification data in treaty verification. To take advantage of new tools and techniques, governments should:

- Map an effective process for societal verification data integration and program management to support future verification systems. Begin to address questions such as:
  - Which agency has the lead?
  - How will the effort intersect with the private sector, the intelligence community, and other potential contributors?
  - How can conclusions be validated using inputs from traditional verification tools?
- Begin international consultations on how future arms reduction agreements may acknowledge and develop rules for the use of societal verification data.
- Explore the possibility of experimenting with cooperative societal verification measures with allies to provide empirical data and lessons for how societal verification may be implemented in the future.
- Start developing rules related to the legal, ethical, and privacy concerns surrounding use of citizen-generated information.

The international technology and policy community should collaborate to develop a technology needs assessment/research and development roadmap to build capacity within government systems. Areas of exploration might include:

- Natural language processing of foreign languages as well as informal and unstructured language, such as slang and terms of art.
- Challenges posed by real-time processing of data versus queries of stored information.
- Identifying key or leading indicators of treaty-proscribed activities around which appropriate queries can be developed.
- Identifying attempts to censor or spoof data, especially where there is knowledge that information is being analyzed.
- Aggregating and integrating signals from multiple sources across platforms and data types to increase confidence.

Governments, in cooperation with outside expert communities, should establish channels to elicit the input of the outside experts community to help build approaches for societal verification:

- Assess capacity and fill gaps to enable contributions by outside experts to societal verification efforts of governments.
- Develop methods and mechanisms to educate expert communities outside the government on existing national verification efforts.
- Develop ways to identify, connect, organize, guide, assist, and reward experts, recognizing that validation and anonymity are not always compatible.
- Create paths to solicit input in a timely manner on potential verification challenges.
- Encourage discussions and cross-checking among external experts, facilitating a two-way information flow to build valuable capacity outside government.

11. Appendix

Societal Verification Considerations in the Wake of the U.S. National Security Agency Revelations

Revelations of National Security Agency (NSA) programs, including the one codenamed "PRISM," highlighted growing insecurities of government access to and use of data generated by individual citizens. While not directly related to societal verification, some key concepts may cross over when governments or individuals assess the potential for its implementation in the future.

EXISTING LAW

The Fourth Amendment

According to the Supreme Court of the United States (SCOTUS), the Fourth Amendment gives U.S. citizens, "a reasonable expectation of privacy." Analysts further this definition: "If you do, say, write or possess something in circumstances suggesting that you expect it to be private, and if society in general would share your expectation, then it's protected."[151] In the 1972 case *US* v. *US District Court*, SCOTUS ruled that the executive branch has no authority to spy on U.S. citizens on U.S. soil without a warrant. However, in the 2012 case *US* v. *Jones*, SCOTUS failed to reach a decision on whether technological surveillance without physical interference violates reasonable expectations of privacy.

The Data Protection Directive

This European Union (EU) directive regulates the processing of personal data within the EU, including data mining of Internet activity. The rules are applicable when the controller of the data processing activities is inside the EU or uses equipment within the EU to process data, thus covering controllers outside the EU processing data coming from the EU.[152] Personal data can only be processed if the data subject is informed of the processing of their personal data, legitimate purposes are specified, or the personal data is not excessively processed.[153]

Other Laws

At least 40 nations have enacted privacy legislation of some sort, protecting internal, overseas, or both types of data transfers, often similar to those listed above.* However, there is no overarching international law protecting Internet privacy.

U.S. EXPERT AND PUBLIC OPINION

U.S. legal and security experts have expressed outrage over PRISM and the general loss of privacy across Internet platforms such as Facebook, Twitter, Skype, and Google. Many experts who endorsed the NSA's actions are security experts who have previously worked in or are currently employed by the army or intelligence services, and lawyers who are affiliated with the United States. However, some polls indicated that the U.S. public sees little problem with the government's monitoring, an important point when considering the future implementation of a societal verification project.

Voicing Outrage

For many experts, the revelations of PRISM and other NSA programs do not present a new fight for privacy, rather a new facet of the struggle. The opinions of experts who focus on privacy issues now overlap with those of lawyers who work to counter the loose privacy codes of various Internet platforms in their concern over the government's surveillance. Neither community is shocked by PRISM, but they now have new evidence to support their positions on privacy rights.[154] These ideals will likely carry over into any discussion of societal verification, which might use similar data mining methods as those of the NSA.

* For a full list of Internet privacy laws, see Information Shield, "International Privacy Laws," accessed April 1, 2014, www.informationshield.com/intprivacylaws.html. Notably absent from this list are Russia and China.

Organizations such as Freedom Watch and the American Civil Liberties Union (ACLU) have filed lawsuits against the Obama Administration and some specific companies for their participation in PRISM. The ACLU lawsuit solely questions the legality of the surveillance program, while Freedom Watch's lawsuit focuses on the possible legal violations of the corporations involved as well as the government itself.

Supporting the Government

Proponents of the NSA surveillance programs compare NSA activities with corporations' data mining. Max Boot, a security expert at the Council on Foreign Relations asserts that companies such as Google, Facebook, Amazon, and Twitter already use the same data-mining tools as the government to cater advertisements to users, and therefore know as much about online activity as the government does. Former NSA director Michael Hayden, NSA chief general Keith Alexander, and retired U.S. Army lieutenant colonel Ralph Peters support this viewpoint and say that there have been far fewer terrorist attacks than expected due to such surveillance methods.[155]

Public Perception

In polls, the U.S. public largely endorsed the surveillance actions taken by the NSA, regardless of the infringement on their privacy. According to a Washington Post-Pew Research Center poll, 62 percent of U.S. Citizens said it was more important for the government to investigate terrorism than it was to protect personal privacy; 45 percent said that the government should be able to monitor everyone's online activity if doing so would prevent terrorist attacks; and 56 percent said that the NSA accessing telephone records through secret court orders was "acceptable."[156]

Public opinion on the issue of government's intrusion on privacy for national security means is important to a societal verification project, as reducing nuclear risks may rank as high as terrorism among societal concerns. Furthermore, the trend in numbers shows that data-mining methods are growing more acceptable in both the governmental and corporate world. If this trend continues, societal verification methods may be publicly accceptable, thus increasing its chances of contributing value as a monitoring method.

INTERNATIONAL PERSPECTIVE ON PRIVACY

Most known international perspectives on privacy come from the EU because of controversies surrounding the NSA surveillance of EU member states and corporate privacy policies. The opinions on privacy presented in three specific cases below may shed light on how EU states and citizens have reacted to unauthorized monitoring, providing possible lessons for the application of societal verification.

NSA Surveillance of EU Member States

Upon learning through Edward Snowden's leaks that the United States has been engaged in widespread spying on European Internet users, state offices, and national officials, the EU threatened to suspend two agreements granting the United States access to European financial and travel data. Although the United States and EU see these agreements as vital tools to fight terrorism, the EU home affairs commissioner, Cecila Malmstrom, wrote two senior U.S. officials warning that if the benefits for citizens could not be verified, the agreements would be in jeopardy.[157]

EU governments have expressed outrage at the revelations. French President Francois Hollande threatened to block negotiations on a transatlantic free trade treaty if the United States did not clarify its activities. German federal prosecutors sought to bring charges against British and U.S. intelligence, as a result of the NSA's phone and Internet surveillance operation in Germany.[158] However, most of the outrage shown by EU leaders has focused on the secrecy and betrayal of trust by the NSA's surveillance, not the tactics per se, showing that they may be open to collaborative use of the same tools in societal verification.

Facebook's Privacy Policy in Europe

Austrian law student Max Schrems has filed multiple complaints in Europe since 2011 regarding Facebook's data practices, claiming that the company does not understand the strict data protection laws on the continent. Founder of the activist group Europe v. Facebook, Schrems asserts that Facebook violates Europeans' privacy by withholding information, illegal under the Data Protection Directive.* Schrems' battle continues amid the revelation that Apple, Facebook, Google, Microsoft, Skype, and Yahoo cooperated with the NSA's PRISM program in violation of EU privacy law. His organization filed complaints with the European data protection authority requesting clarification

* Schrems requested his files from Facebook under the Data Protection Directive guarantee that Europeans have the right to access all information a company knows about them. After withholding certain information, Facebook claimed that it was a trade secret, but many criticized Facebook for claiming that users' data was the company's intellectual property.

on whether an EU-based company can forward user data to an intelligence agency.[159] This complaint is supported by the ACLU and other activist organizations both within and outside Europe.[160]

Controversy over Google's Privacy Policy

Privacy watchdogs in the United Kingdom, Germany, and Italy have ordered Google to rewrite its privacy policy or face legal sanctions. This warning comes after the change in Google's privacy policy in March 2012, when the company unified each individual's data across YouTube, Maps, Shopping, Mail, and Search. Google was criticized in Europe over its collection of wi-fi data and has been questioned by European privacy authorities and U.S. legislators about the data protection implications of Google Glass, which allows users to take video and pictures without the subjects' knowledge.[161] While the effect of these complaints on Google's privacy policies are so-far unknown, privacy issues are growing in the EU.

12. Endnotes

[1] See CFR Task Force, "Defending an Open, Global, Secure, and Resilient Internet," Council on Foreign Relations, June 2013, accessed April 1, 2014, www.cfr.org/cybersecurity/defending-open-global-secure-resilient-internet/p30836. Global Internet traffic has also increased from 100 gigabytes per day in 1992, to 100 gigabytes per second in 2002, to 12,000 gigabytes per second in 2012. Forecasts are that Internet traffic will increase to 35,000 gigabytes per second by 2017. See Cisco, "The Zettabyte Era—Trends and Analysis," white paper, May 29, 2013.

[2] Data compiled from University of North Caroline at Pembroke, "The Brief History of Social Media," accessed September 24, 2013, www.uncp.edu/home/acurtis/NewMedia/SocialMedia/SocialMediaHistory.html; Jeff Dunn, "A Detailed History of Social Media," Edudemic, July 1, 2013, accessed September 24, 2013, www.uncp.edu/home/acurtis/NewMedia/SocialMedia/SocialMediaHistory.html.

[3] Cisco, "The Zettabyte Era."

[4] Business Wire, "Smartphones Expected to Outship Feature Phones for First Time in 2013, According to IDC," March 4, 2013, accessed September 25, 2013, www.businesswire.com/news/home/20130304005403/en/Smartphones-Expected-Outship-Feature-Phones-Time-2013.

[5] Business Wire, "Smartphones."

[6] Seymour Melman, ed., "Inspection by the People: Mobilization of Public Support," in *Excerpts from Inspection for Disarmament* (New York: Columbia University Press, 1958), 39.

[7] Joseph Rotblat, "Toward a Nuclear Weapon-Free World: Societal Verification," *Security Dialogue* 23, no. 51 (1992), 52.

[8] Kirk C. Bansak, "Trust, but Socially Verify," *Bulletin of the Atomic Scientists*, August 10, 2012, 2.

[9] Dieter Deiseroth, "Societal Verification: Wave of the Future?" *Societal Verification* (London: Verification Research Training, and Information Centre, 2000), 265.

[10] J.J. Fahie, *A History of Wireless Telegraphy* (New York: Dodd, Mead, and Co., 1901).

[11] Leonard C. Bruno, "The Invention of the Telegraph," U.S. Library of Congress, accessed April 1, 2014, memory.loc.gov/ammem/sfbmhtml/sfbmtelessay.html.

[12] Arthur Wilson, *The Living Rock: The Story of Metals Since Earliest Times and Their Impact on Civilization* (Cambridge: Woodhead Publishing, 1994), 203.

[13] David Paul Nickles, *Under the Wire: How the Telegraph Changed Diplomacy* (Cambridge: Harvard University Press, 2003).

[14] Yahya A. Dehqanzada and Ann M. Florini, *Secrets for Sale: How Commercial Satellite Imagery Will Change the World*, (Washington, DC: Carnegie Endowment for International Peace, 2000) http://www.carnegieendowment.org/files/FINALreport.pdf.

[15] T. White, "United States Early Radio History," United States Early Radio History, accessed April 1, 2014, earlyradiohistory.us/.

[16] White, "Early Radio."

[17] D.A. Johnson, "The Radio Legacy of the RMS Titanic," accessed April 9, 2014, www.avsia.com/djohnson/titanic.html.

[18] D. Mankowski and R. Jose, "MBC Flashback: The 70th Anniversary of FDR's Fireside Chats," accessed April 1, 2014, www.museum.tv/index.htm.

[19] C. Fenwick, "The Use of the Radio as an Instrument of Foreign Propaganda," *The American Journal of International Law* 32, no. 2 (1938): 339–343.

[20] N. Snow and P.M. Taylor, "The Revival of the Propaganda State: U.S. Propaganda at Home and Abroad since 9/11," *International Communication Gazette* 68, no. 5–6 (2006): 389–407.

[21] C.E. Scott, "The History of the Radio Industry in the United States to 1940," *Economic History Services*, accessed April 1, 2014, eh.net/?s=The+History+of+the+Radio+Industry+in+the+United+States+to+1940+.

[22] E. Katz and P.F. Lazarsfeld, *Personal Influence: The Part Played by People in the Flow of Mass Communications* (Glencoe, IL: Free Press, 1955).

[23] See U.S. Geological Survey, "Earthshots: Satellite Images of Enviromental Change—Chernobyl, Ukraine," accessed April 1, 2014, earthshots.usgs.gov/earthshots/Chernobyl#ad-image-6.

[24] Laurie J. Schmidt, "New Tools for Diplomacy: Remote Sensing Use in International Law," *Earth Observatory*, January 12, 2001, accessed April 1, 2014, earthobservatory.nasa.gov/Features/Diplomacy/.

[25] Bhupendra Jasani and Toshibomi Sakata, eds., *Satellites for Arms Control and Crisis Monitoring* (Oxford: Oxford University Press, 1987); Michael Krepon, Peter D. Zimmerman, Leonard S. Spector, and Mary Umberger, eds., *Commercial Observation Satellites and International Security* (New York: St. Martin's Press, 1990).

[26] Yahya A. Dehqanzada and Ann M. Florini, *Secrets for Sale: How Commercial Satellite Imagery Will Change the World* (Washington, DC: Carnegie Endowment for International Peace, 2000); John C. Baker, Kevin M O'Connell, and Ray A. Williamson, eds., *Commercial Observation Satellites: At the Leading Edge of Global Transparency* (Santa Monica, CA: Rand, 2001); U.S. Central Intelligence Agency, *Project Epoch: Commercial Imagery Support to Transnational Intelligence Issues: Proof of Concept* (Washington, DC: Space Imaging, 1998).

[27] Rose Gottemoeller, "From the Manhattan Project to the Cloud: Arms Control in the Information Age," Sidney Drell Lecture, Stanford University, October 27, 2011, accessed April 14, 2014, http://www.state.gov/t/avc/rls/176331.htm.

[28] Paul Levinson, *New New Media* (New York: Pearson Education, 2013).

[29] See en.wikipedia.org/wiki/List_of_social_networking_websites.

[30] Haewoon Kwak, Changhyun Lee, Hosung Park, and Sue Moon, "What Is Twitter, A Social Network or a News Media?" Paper presented at the proceeedings of the 19th International Conference on the World Wide Web, Raleigh, NC, April 26–30, 2010.

[31] Danah M. Boyd and Nicole B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* 13, no. 1 (2007): 210–230.

[32] J. Ibrahim, R. Rajagopalan, and I. Ibrahim, "The Potential and Pitfalls of Societal Verification," accessed April 9, 2014, thebulletin.org/potential-and-pitfalls-societal-verification.

[33] "Teenage Super Sleuth, 16, Tracks Burglar Down in ONE HOUR on Facebook after Raid on Home and Gets Him Jailed For Two Years," *Daily Mail*, November 2, 2012.

[34] R. Bond, C. Fariss, J. Jones, A. Kramer, C. Marlow, J. Settle, and J. Fowler, "A 61-Million-Person Experiment in Social Influence and Political Mobilization," *Nature 489* (September 13, 2012): 295–298.

[35] Malcolm Gladwell, "Small Change: Why the Revolution Won't Be Tweeted," *The New Yorker*, October 4, 2010.

[36] Kwak, Lee, Park, and Moon, "What Is Twitter?"

[37] Meeyoung Cha, Hamed Haddadi, Fabrício Benevenuto, and Krishna P. Gummandi, "Measuring User Influence in Twitter: The Million Follower Fallacy," paper presented at the Fourth International AAAI Conference on Weblogs and Social Media, Washington, DC, May 23–26, 2010.

[38] Andranick Tumasjan, Timm O. Sprenger, Philipp G. Sandner, and Isabell M. Welpe, "Predicting Elections with Twitter: What 140 Characters Reveal about Political Sentiment," paper presented at the proceedings of the Fourth International AAAI Conference on Weblogs and Social Media, Washington, DC, May 23–26, 2010.

[39] Johan Bollen, Huina Mao, and Xiaojun Zeng, "Twitter Mood Predicts the Stock Market," *Journal of Computational Science* 2, no. 1 (2011).

[40] Brendan O'Connor, Ramnath Balasubryamanyam, Bryan R. Routledge, and Noah A. Smith, "From Tweets to Polls: Linking Test Sentiment to Public Opinion Time Series," paper presented at the proceedings of the Fourth International AAAI Conference on Weblogs and Social Media, Washington, DC, May 23–26, 2010.

[41] Gary King, Jennifer Pan, and Molly Roberts. "How Censorship in China Allows Government Criticism but Silences Collective Expression," American Political Science Association 2012 annual meeting paper, 2012.

[42] H. Gao, G. Barbier, and R. Goolsby, "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief," *Intelligent Systems* 26, no. 3 (2011).

[43] See *Safecast* blog, accessed April 1, 2014, blog.safecast.org/maps/.

[44] See, e.g., Joshua Rutkowski, "Satellite Imagery Analysis at the International Atomic Energy Agency," lecture at United Nations Geographic Information Working Group (UNGIWG), March 29, 2012, accessed April 1, 2014, ungiwg.ctbto.org/keynotes/satellite-imagery-analysis-international-atomic-energy-agency; see also: Bhupendra Jasani, Irmgard Niemeyer, Sven Nussbaum, Bernd Richter, Gotthard Stein, eds., *International Safeguards and Satellite Imagery: Key Features of the Nuclear Fuel Cycle and Computer-based Analysis* (Berlin: Springer-Verlag, 2009).

[45] See, e.g., Ian B. Murphy, "Crowdsourcing Speeds Satellite Monitoring of Syrian Crisis," Data Informed, accessed April 9, 2014, data-informed.com/crowdsoucing-speeds-satellite-monitoring-of-syrian-crisis/.

[46] See, e.g., "Satellite Imagery Reveals Predator-Prey Behavior in Coral Reefs," *Earth Imaging Journal*, 2011, accessed April 1, 2014, eijournal.com/2011/satellite-imagery-reveals-predator-prey-behavior-in-coral-reefs.

[47] See, e.g., United Nations Institute for Training and Research, www.unitar.org/unosat/.

[48] Twitter (twitter.com), Flickr (www.flickr.com), Panoramio, (www.panoramio.com), and SketchUp (sketchup.google.com).

[49] See, e.g., Ogle Earth, ogleearth.com/.

[50] See, e.g., Wikimapia, wikimapia.org/.

[51] See Satellite Sentinel Project, accessed April 1, 2014, www.satsentinel.org/.

[52] Disaster Recovery and Intergovernmental Affairs Subcommittee, Understanding the Power of Social Media as a Communications Tool in the Aftermath of Disasters, May 2011, accessed April 9, 2014, www.hsgac.senate.gov/subcommittees/disaster-recovery-and-intergovernmental-affairs/hearings/understanding-the-power-of-social-media-as-a-communications-tool-in-the-aftermath-of-disasters.

[53] See Ushahidi, accessed April 1, 2014, www.ushahidi.com/products/ushahidi-platform.

[54] See Waze, accessed April 1, 2014, www.waze.com/.

[55] See City of Boston, "City Releases Prototype of Smart Phone App that Detects Potholes," press release, February 9, 2011, accessed April 1, 2014, www.cityofboston.gov/news/default.aspx?id=4979; http://www.cityofboston.gov/cable/video_library.asp?id=1875.

[56] See GammaPix, accessed April 1, 2014, www.gammapix.com.

[57] David M. Blei, Andrew Y. Ng, and Michael I. Jordan, "Latent Dirichlet Allocation," *Journal of Machine Learning Research* 3 (March 1, 2003): 993–1022.

[58] Killian Thiel, Tobias Kotter, Michael Berthold, Rosaria Silipo, and Phil Winters, "Creating Useable Customer Intelligence from Social Media Data: Network Analytics Meets Text Mining," white paper, KNIME, Zurich, 2012.

[59] Abdelhalim Rafrafi, Vincent Guige, and Patrick Gallinari, "Coping with Document Frequency Bias in Sentiment Classification," presented at the Sixth International AAAI Conference on Weblogs and Social Media, Dublin, June 4–8, 2012.

[60] See Munmun De Choudhury, Michael Gamon, and Scott Counts, "Happy, Nervous, or Surprised? Classification of Human Affective States in Social Media," presented at the Sixth International AAAI Conference on Weblogs and Social Media, Dublin, June 4–8, 2012; Jed R. Brubaker, Funda Kivran-Swaine, Lee Taber, and Gillian R . Hayes, "Grief-Stricken in a Crowd: The Language of Bereavement and Distress in Social Media," presented at the Sixth International AAAI Conference on Weblogs and Social Media, Dublin, June 4–8, 2012.

[61] Lora Weiss, Erica Briscoe, Heather Hayes, Olga Kemenova, Sim Harbert, Fuxin Li, Guy Lebanon, Chris Stewart, Darby Miller Steiger, and Dan Foy, "A Comparative Study of Social Media and Traditional Polling in the Egyptian Uprising of 2011," in *Social Computing, Behavioral-Cultural Modeling, and Prediction* (Berlin: Springer-Verlag, 2013): 303–310.

[62] Przemyslaw A. Grabowicz, Jose J. Ramasco, Esteban Moro, Josep M. Pujol, and Victor M. Eguiluz, "Social Features of Online Networks: The Strength of Intermediary Ties in Online Social Media," *PLOS ONE* 7, no. 1 (January 11, 2012).

[63] See Arms Control Wonk, ed. Jeffrey Lewis, accessed April 1, 2014, armscontrolwonk.com.

[64] Mark S. Granovetter, "The Strength of Weak Ties," *American Journal of Sociology* 78, no. 6 (1973): 1360–1380.

[65] Natasha Singer, "When the Data Struts Its Stuff," *The New York Times*, April 2, 2011.

[66] Jean Mark Gawron, Dipak Gupta, Kellen Stephens, Ming-Hsiang Tsou, Brian Spitzberg, and Li An, "Using Group Membership Markers for Group Identification," presented at the Sixth International AAAI Conference on Weblogs and Social Media, Dublin, June 4–8, 2012.

[67] Jennifer Golbeck, Cristina Robles, and Karen Turner, "Predicting Personality with Social Media," presented at ACM CHI Conference on Human Factors in Computing Systems, Vancouver, May 7–12, 2011.

[68] D. Scott Appling, Erica J. Briscoe, Heather Hayes, and Rudolph L. Mappus, "Towards Automated Personality Identification Using Speech Acts," workshop on computational personality recognition, Seventh International AAAI Conference on Weblogs and Social Media, Boston, July 11, 2013.

[69] Sitaram Asur and Bernardo A. Huberman, "Predicting the Future with Social Media," March 29, 2010, arXiv:1003.5699v1, accessed November 29, 2012.

[70] J. Dimond, "Feminist HCI for Real: Designing Technology in Support of a Social Movement." (dissertation, Georgia Institute of Technology, Atlanta, Georgia, 2012).

[71] J. Tang, M. Cebrian, N. Giacobe, H. Kim, T. Kim, and D. Wickert, "Reflecting on the DARPA Red Balloon Challenge," *Communications of the ACM* 54, no. 4 (April 2011).

[72] M. Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age* (Cambridge, UK: Polity Press, 2012).

[73] Castells, *Networks*.

[74] Dimond, "Feminist HCI."

[75] P.M. Haas, "Introduction: Epistemic Communities and International Policy Coordination," *International Organization* 46, no. 1 (1992): 1–35.

[76] E. Adler, "The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control," *International Organization* 46, no. 1 (1992): 101–145.

[77] E. Wenger, *Communities of Practice: Learning, Meaning, and Identity* (Cambridge: Cambridge University Press, 1999).

[78] John C. Thomas, Wendy A. Kellogg, and Thomas Erickson, "The Knowledge Management Puzzle: Human and Social Factors in Knowledge Management," *IBM Systems Journal* 40, no. 4 (2001): 863–884.

[79] D. MacKenzie and G. Spinardi, "Tacit Knowledge, Weapons Design, and the Uninvention of Nuclear Weapons," *American Journal of Sociology* 101, no. 1 (1995): 44–99.

[80] S. Postrel, "Islands of Shared Knowledge: Specialization and Mutual Understanding in Problem-Solving Teams," *Organization Science* 13, no. 3 (2002): 303–320.

[81] Personal conversation with author, Warrenton, VA, February 13, 2013.

[82] Miller McPherson, Lynn Smith-Lovin, and James M. Cook, "Birds of a Feather: Homophily in Social Networks," *Annual Review of Sociology* 27 (2001): 415–444; Sinan Aral, Lev Muchnik, and Arun Sundararajan, "Distinguishing Influence-Based Contagion from Homophily-Driven Diffusion in Dynamic Networks," *Proceedings of the National Academy of Sciences of the United States of America*, 106, no. 51 (2009): 21544–21549; Shaomei Wu, Jake M. Hofman, Winter A. Mason, and Duncan J. Watts, "Who Says What to Whom on Twitter," Proceedings of the 20th International World Wide Web Conference, Hyderabad, India, March 28–April 1, 2011.

[83] Kwak, Lee, Park, and Moon, "What is Twitter?"

[84] E. Von Hippel, *The Sources of Innovation* (New York: Oxford University Press, 1988).

[85] S. Wasserman and K. Faust, *Social Network Analysis: Methods and Applications* (Cambridge: Cambridge University Press, 1994).

[86] Katsuhide Fujita, Yuya Kajikawa, Junichiro Mori, and Ichiro Sakata, "Detecting Research Fronts Using Different Types of Weighted Citation Networks," *Journal of Engineering and Technology Management* (August 22, 2013).

[87] M.E. Newman, "Scientific Collaboration Networks. I. Network Construction and Fundamental Results," *Physical Review* E 64, no. 1 (2001).

[88] Alex Marin, Bin Zhang, and Mari Ostendorf, "Detecting Forum Authority Claims in Online Discussions," Proceedings of the Workshop on Language in Social Media, Portland, OR, June 23, 2011, 39–47.

[89] D.C. Brabham, "Crowdsourcing as a Model for Problem Solving an Introduction and Cases," *Convergence: The International Journal of Research into New Media Technologies* 14, no. 1 (2008): 75–90.

[90] D.C. Brabham, "The Myth of Amateur Crowds," *Information, Communication & Society* 15, no. 3 (2012): 394–410.

[91] Eliot Van Buskirk, "How the Netflix Prize Was Won," *Wired*, September 22, 2009.

[92] J.A. Botía and D. Charitos, "Pedestrian Navigation and Shortest Path: Preference versus Distance," Workshop Proceedings of the Ninth International Conference on Intelligent Environments, Athens, July 18–19, 2013.

[93] Karim Lakhani, Lars Bo Jeppesen, Peter A. Lohse, and Jill A. Panetta, "The Value of Openness in Scientific Problem Solving" (working paper 07-050, Harvard Business School, Boston, 2006.)

[94] W. Mason and D.J. Watts, "Financial Incentives and the Performance of Crowds," *ACM SigKDD Explorations Newsletter* 11, no. 2 (2010): 100–108.

[95] Thomas W. Malone, Robert Laubacher, and Chrysanthos Dellarocas, "Harnessing Crowds: Mapping the Genome of Collective Intelligence," MIT Sloan Research Paper no. 4732-09, Cambridge, MA, February 3, 2009.

[96] A. Armstrong and J. Hagel III, "The Real Value of Online Communities," *Harvard Business Review* 74, no. 3 (1996): 134–141.

[97] Patrick Bateman, Peter Gray, and Brian Butler, "Community Commitment: How Affect, Obligation, and Necessity Drive Online Behaviors," Twenty-Seventh International Conference on Information Systems, Milwaukee, 2006.

[98] G. Camponovo, *Motivations in Virtual Communities: A Literature Review* (Reading, UK: Academic Conferences International, 2011).

[99] See "Tag Challenge," accessed April 1, 2014, www.tag-challenge.com/; see also "DARPA Network Challenge," accessed April 1, 2014, archive.darpa.mil/networkchallenge/.

[100] See http://scailab.media.mit.edu/crowdscanner/.

[101] U.S. Department of State Announces the Winners of the "Innovation in Arms Control Challenge," March 4, 2013, http://www.state.gov/r/pa/prs/ps/2013/03/205617.htm.

[102] Office of Management and Budget, Digital Government: Building a 21st Century Platform to Better Serve the American People, May 23, 2012, accessed April 1, 2014, www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf.

[103] SDL Government, accessed April 22, 2014, www.sdlgov.com.

[104] David Talbot, "Viral Phone Game Helps Illiterate Pakistanis Find Job Listings," *MIT Technology Review*, March 13, 2013.

[105] Sugata Mitra, "Build a School in the Cloud," TED Talks, February 2013, accessed April 1, 2014, www.ted.com/talks/sugata_mitra_build_a_school_in_the_cloud.html.

[106] Broadcasting Board of Governors, "Nigeria Media Use 2012," white paper, August 20, 2012, accessed April 1, 2014, www.bbg.gov/wp-content/media/2012/08/gallup-nigeria-brief.pdf.

[107] Open Source Center, "The Google Controversy—Two Years Later," report, July 30, 2008, accessed April 1, 2014, www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB404/docs/23.pdf.

[108] Open Source Center, "Google Controversy."

[109] Roy M. Stanley II, *To Fool A Glass Eye: Camouflage versus Photoreconnaissance in World War II* (Washington, DC: Smithsonian Institution Press, 1998); Seymour Reit, *Masquerade: the Amazing Camouflage Deceptions of World War II* (New York: New American Library, 1978).

[110] Andre Oboler, Kristopher Welsh, and Lito Cruz, "The Danger of Big Data: Social Media as a Computational Social Science," *First Monday* 17, no. 2 (July 2, 2012), accessed April 1, 2014, firstmonday.org/ojs/index.php/fm/article/view/3993.

[111] See National Public Radio (NPR) Ethics Handbook, "Social Media," February 25, 2012, accessed April 1, 2014, ethics.npr.org/tag/social-media/.

[112] ESOMAR World Research, "ESOMAR Guidelines of Social Media Research," July 2011, accessed April 1, 2014, www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR-Guideline-on-Social-Media-Research.pdf.

[113] CASRO, "Social Media Research Guidelines," October 17, 2011, accessed April 1, 2014, c.ymcdn.com/sites/www.casro.org/resource/resmgr/docs/social_media_research_guidel.pdf.

[114] Titles 10, 22, 28 Part II and 50 of the U.S. Code govern the U.S. armed forces, the Department of State, Department of Justice, and national defense (including the intelligence community), respectively.

[115] Aspects of this were considered as early as the 1950s. See, e.g., L.C. Bohn, "Non-Physical Inspection Techniques," in Donald G. Brennan, ed., *Arms Control, Disarmament and National Security* (New York: George Braziller, 1961), 350; L.B. Sohn and G. Clark, *World Peace through World Law* (Cambridge: Harvard University Press, 1960).

[116] Gregory Kulacki, "Research in the Internet Age: Karber and China's Nuclear Arsenal," Union of Concerned Scientists, November 30, 2011, accessed April 1, 2014, allthingsnuclear.org/research-in-the-internet-age-karber-and-chinas/.

[117] Juan Carlos Perez, "Facebook's Beacon More Intrusive than Previously Thought," *PC World*, November 30, 2007, accessed April 1, 2014, http://www.pcworld.com/article/140182/article.html.

[118] Oboler, Welsh, and Cruz, "Danger of Big Data."

[119] Charles Duhigg, "How Companies Learn Your Secrets," *The New York Times*, February 16, 2012.

[120] Duhigg, "Learn Your Secrets."

[121] Oboler, Welsh, and Cruz, "Danger of Big Data."

[122] K.J. O'Brien, "Firms Brace for New European Data Privacy Law," *The New York Times*, May 13, 2013.

[123] Activities conducted for authorized intelligence (Title 50 of the U.S. Code [USC]) or law-enforcement purposes (Title 28 USC) may have a very different set of privacy-related requirements than something done to support public diplomacy (Title 22 USC).

[124] U.S. Export.Gov, "U.S.-EU Safe Harbor Overview," accessed April 1, 2014, export.gov/safeharbor/eu/eg_main_018476.asp.

[125] A. Sullivan, "Protecting the Leakers," *The Dish* (blog), May 16, 2013, accessed April 1, 2014, dish.andrewsullivan.com/2013/05/16/protecting-the-leakers/.

[126] A. Narayanan and V. Shmatikov, "De-Anonymizing Social Networks," Proceedings of 30th IEEE Symposium on Security and Privacy, Oakland, 2009, 173–187.

[127] John Poindexter, at DARPATech 2002 Conference, Anaheim, CA, August 2, 2002, http://www.fas.org/irp/agency/dod/poindexter.html.

[128] ESOMAR, "ESOMAR Guidelines."

[129] Jodi Dean, "Communicative Capitalism: Circulation and the Foreclosure of Politics," *Cultural Politics* 1, no. 1 (2005): 51–74.

[130] Clay Shirky, "The Political Power of Social Media," *Foreign Affairs* 90, no. 1 (2011): 28–41.

[131] D. Fahrenthold and C. Dewey, "Backpack Brothers an Example of the Drawbacks to Internet Sleuthing," *The Washington Post*, April 18, 2013.

[132] Gladwell, "Small Change."

[133] U.S. Department of Defense, *Dictionary of Military and Associated Terms* (Washington, DC: Joint Chiefs of Staff, 2010), amended through November 15, 2012.

[134] Reuters, "UPDATE 3-New Broader Russian Treason Law Alarms Putin Critics," Nov 14, 2012, accessed April 1, 2014, www.reuters.com/article/2012/11/14/russia-treason-idUSL5E8ME4Y620121114.

[135] The Law of the People's Republic of China on Guarding State Secrets (中□人民共和国保守国家秘密法), accessed April 1, 2014, www.gov.cn/flfg/2010-04/30/content_1596420.htm.

[136] Criminal Law of The People's Republic of China (2011) (中□人民共和国刑法[2011年最新修□版]), accessed April 1, 2014, www.china.com.cn/policy/txt/2012-01/14/content_24405327.htm.

[137] P.J. Harbour, "The Emperor of All Identities," *The New York Times*, December 19, 2012.

[138] Google, "A Second Spring of Cleaning," Official Google Blog, March 13, 2013, accessed April 9, 2014, googleblog.blogspot.com/2013/03/a-second-spring-of-cleaning.html.

[139] Statement of Rights and Responsibilities," https://www.facebook.com/legal/terms., accessed April 2014.

[140] "Twitter Privacy Policy," https://twitter.com/privacy, accessed April 2014.

[141] J. Battelle, *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture* (New York: Portfolio, 2005).

[142] M. Ingram, "'Twitter Killed My Business': An Inside Look at the Ecosystem Crackdown—Tech News and Analysis," Gigaom, September 7, 2012, accessed April 9, 2014, gigaom.com/2012/09/07/twitter-killed-my-business-an-inside-look-at-the-ecosystem-crackdown/.

[143] NodeXL (2013). Twitter API 1.1 and Excel 2013.

[144] Google, "Second Spring."

[145] P. Ujjainwalla, "The Death of the Google Shopping API | Modern Retail Pricing," *360pi.com* (blog), April 24, 2013, accessed April 9, 2014, blog.360pi.com/the-death-of-the-google-shopping-api/.

[146] Google, "Transparency Report," accessed April 9, 2014, www.google.com/transparencyreport/removals/government/.

[147] W. Dobson, "Needles in a Haystack," *Newsweek*, August 6, 2010.

[148] Shirky, "Political Power of Social Media."

[149] Shirky, "Political Power of Social Media."

[150] J. Obar, P. Zube, and C. Lampe, "Advocacy 2.0: An Analysis of How Advocacy Groups in the United States Perceive and Use Social Media as Tools for Facilitating Civic Engagement and Collective Action," *Journal of Information Policy* 2 (2012): 1–25.

[151] Charles Lane, "Snowden Case Shows Need to Revisit Privacy Laws," *The Washington Post*, June 17, 2013.

[152] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31, art. 4, accessed April 1, 2014, eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[153] Directive 95/46/EC, art. 6, 7, 10, 11.

[154] Harry R. Lewis, "Who Cares About Surveillance?" *Bits and Pieces* (blog), June 13, 2013, accessed April 1, 2014, harry-lewis.blogspot.com/2013/06/who-cares-about-prism.html.

[155] Ralph Peters, "Spy vs. Lie," *New York Post*, June 16, 2013; Jonathan Masters and Greg Bruno, "U.S. Domestic Surveillance," backgrounder, Council on Foreign Relations, June 13, 2013, accessed April 1, 2014, www.cfr.org/intelligence/us-domestic-surveillance/p9763; Eli Lake, "Former NSA Director Michael Hayden Responds to Edward Snowden Claim," *Daily Beast*, June 12, 2013, accessed April 1, 2014, www.thedailybeast.com/articles/2013/06/12/former-nsa-director-michael-hayden-responds-to-edward-snowden-claim.html.

[156] Jon Cohen, "Most Americans Back NSA Tracking Phone Records, Prioritize Probes over Privacy," *The Washington Post*, June 10, 2013.

[157] Adrian Croft, "EU Threatens to Suspend Data Agreements with US, Citing Privacy Concerns," *The Christian Science Monitor*, July 5, 2013.

[158] Damien McElroy, Bruno Waterfield, and Tom Parfitt, "Francois Hollande Tells the US to Stop Eavesdropping on Europe If It Wants Progress on Trade Deal," *The Telegraph*, July 1, 2013; "Partner Spionieren Einander Nicht Aus," Frankfurter Allgemeine Politik, June 30, 2013, accessed April 2, 2014, www.faz.net/aktuell/politik/ausland/nsa-abhoeraffaere-partner-spionieren-einander-nicht-aus-12265778.html.

[159] Europe-v-Facebook.org, "NSA/PRISM: Legal Actions against European Subsidiaries of Facebook, Apple, Microsoft, Skype, and Yahoo Filed," update, June 26, 2013, accessed April 2, 2014, www.europe-v-facebook.org/PRISM_PA_en.pdf.

[160] Jay Stanley, "Activists Leverage Stronger EU Privacy Laws to Seek More Information on PRISM," American Civil Liberties Union, June 27, 2013, accessed April 2, 2014, www.aclu.org/blog/national-security-technology-and-liberty/activists-leverage-stronger-eu-privacy-laws-seek-more.

[161] Charles Arthur, "European Watchdogs Order Google to Rewrite Privacy Policy or Face Legal Action," *The Guardian*, July 5, 2013.

NTI

BUILDING A SAFER WORLD

ABOUT THE NUCLEAR THREAT INITIATIVE

The Nuclear Threat Initiative (NTI) is a non-profit, non-partisan organization with a mission to strengthen global security by reducing the risk of use and preventing the spread of nuclear, biological, and chemical weapons and to work to build the trust, transparency, and security that are preconditions to the ultimate fulfillment of the Non-Proliferation Treaty's goals and ambitions.

Founded in 2001 by former U.S. Senator Sam Nunn and CNN founder Ted Turner, NTI is guided by a prestigious, international board of directors. Joan Rohlfing serves as president.

Innovating Verification: New Tools & New Actors to Reduce Nuclear Risks

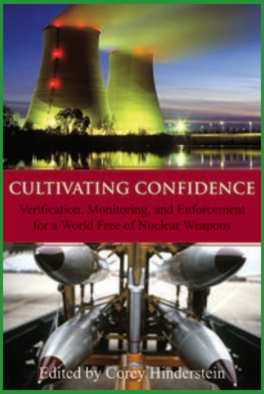
Redefining Societal Verification

> "Progress must be made through a joint enterprise among nations, recognizing the need for greater cooperation, transparency, and verification to create the global political environment for stability and enhanced mutual security."
>
> ~ George P. Shultz, William J. Perry, Henry A. Kissinger, and Sam Nunn,
> "Deterrence in the Age of Nuclear Proliferation,"
> *The Wall Street Journal,* March 7, 2011

The Verification Pilot Project of the Nuclear Threat Initiative convened more than 40 technical and policy experts from around the world to develop recommendations for new approaches to verification that could enable future progress on arms reductions and prompt near-term progress on non-proliferation and nuclear security.

Innovating Verification: New Tools & New Actors to Reduce Nuclear Risks is a report series with the results of the project. It calls for the international community to fundamentally rethink the design, development, and implementation of arms control verification. An international initiative pursued with creativity, broad participation from states with and without nuclear weapons, and a sense of urgency and common purpose could make a significant contribution to global security.

This series of reports builds on *Cultivating Confidence: Verification, Monitoring, and Enforcement for a World Free of Nuclear Weapons* (Nuclear Threat Initiative, 2010), which outlined key issues that states need to address to ensure that nuclear weapons reductions can proceed in a safe and transparent manner.


CULTIVATING CONFIDENCE
Verification, Monitoring, and Enforcement for a World Free of Nuclear Weapons
Edited by Corey Hinderstein

Other publications in the Cultivating Confidence Series include *Innovating Verification: Overview, Verifying Baseline Declarations of Nuclear Warheads and Materials*, and *Building Global Capacity*.

NTI
BUILDING A SAFER WORLD

www.nti.org