Big Data and International Relations

*Andrej Zwitter**

From November 26 to 29, 2008, ten heavily armed members of Lashkar-e-Taiba (LeT), a Kashmiri separatist group, attacked several public sites in Mumbai, India, with automatic weapons and grenades, killing 164 people and wounding three hundred. This was one of the first known instances of terrorists employing powerful search algorithms such as Twitter's or the link analysis used in Google's PageRank system, which allowed LeT members to access information from massive data pools in real-time. During the attacks, an LeT operations center based in Pakistan communicated with the terrorists via sattelite and GSM phones to provide them with open-source intelligence. From the operations center, LeT members data mined the Internet and social media, tapping into the power of Big Data to provide the attackers with an intelligence advantage over Indian law enforcement agencies. The attackers were thereby kept up to date on the status of the Indian government's response and even received personal profiles of the hostages they took in the Taj Mahal Palace hotel.[1]

Ironically, counterterrorism agencies are relying on the same technological advances to stop similar attacks from occurring. For example, the U.S. military is developing drones that, empowered by the combination of facial recognition software and vast databases of face-tagged photos, are able to identify individuals even in crowds—leading to what experts call hyperpersonalized warfare.[2] Furthermore, using data-mining techniques, trend spotting, and sentiment analysis, experts in the area of predictive policing and intelligence analysis are hoping to distill the indicators and to identify the anomalies that would help predict terrorist attacks, counteract organized crime groups, and, at the same time, save resources—and potentially lives—by employing targeted interventions.

*This essay was produced as part of the cooperation between the Austrian Institute for International Affairs and the Danube University Krems, Austria.

Ethics & International Affairs, 29, no. 4 (2015), pp. 377–389.

doi:10.1017/S0892679415000362

Big Data increasingly affects politics in manifold ways. With the ascendance of cyberspace as an important domain of daily activity, international politics has already experienced technology-driven change. Big Data unveils new dimensions to these changes, which we as political scientists and observers of international affairs are only now beginning to comprehend. It changes power distributions and thereby some basic assumptions of international relations theory, and its analytics will increasingly inform international relations research and policymaking. It has created both new opportunities and threats in areas such as humanitarian aid, development, and international peace and security. As hardware becomes better and cheaper, and as open-source software and database search and analysis services become more widely available, the power of Big Data is also increasingly at the disposal of small enterprises and individuals. Its ascendance in all aspects of social and political life has also sharpened important questions about global Internet governance.

What Is Big Data?

Big Data refers to the enormous amounts of data that, using sophisticated analytics techniques, can be mined for information in order to reveal patterns and spot trends and correlations. A key idea behind the concept is that the sheer volume of data allows users to discover information—specifically, correlations and patterns—that would not be available by looking at smaller samples. It also relates to the enhanced ability to extract information from, and interpret, massive amounts of unstructured data. Another key idea is that Big Data is updated in near real-time. The most important features relevant to understanding Big Data are known as "the three Vs," which are:[3]

- Volume: Data today exists in massive amounts, which can be measured in petabytes [10^{15} bytes], exabytes [10^{18} bytes], and zetabytes [10^{21} bytes]. Soon, it will even be measured in yottabytes [10^{24}], one of which equals 250 trillion digital video disks. According to Rick Smolan and Jennifer Erwitt, from the beginning of history until 2011, five billion gigabytes were produced; in 2015 this amount is produced every ten seconds.[4]
- Velocity: The speed of data creation and its collection now approaches real-time. This concerns not only questions of bandwidth (megabyte and gigabyte upload and download capabilities) but also of implementing

https://doi.org/10.1017/S0892679415000362 Published online by Cambridge University Press

information-technology architecture solutions that can cope with data in near real-time.

- Variety: Data exists in structured and unstructured forms and in different formats and units of analysis, including documents, emails, social media messages, YouTube videos, pictures, audio, radio-frequency identification chips,[5] satellite imagery, sky cartography, DNA sequencing, phone-network call data, and cell phone GPS signals. Furthermore, it can be categorized depending on its source: for example, there is self-generated data, data collected (mostly in automatized ways) from the web (known as data scraping), and data retrieved from other outside sources.

Some authors add a number of other features that are potentially, but not necessarily, present in Big Data:

- Veracity: This fourth V encompasses all sorts of methodological questions about the reliability and validity of data and its sources. For example, possible biases can be generated by the form of collection (do sentiment analyses generated from a certain region based on Twitter feeds actually express the sentiments of that region, or only those of Twitter users from that region?), and the form of data preparation (for example, by removing duplicates, completing partial entries, aggregating results, and so on).
- Value: Oracle, for example, considers Big Data to be of low value density; that is, the data received and collected requires much processing before value can be extracted from it.[6]
- Correlations: Algorithms that analyze Big Data emphasize correlations over causation for the use of predictions and for social engineering, that is, the manipulation of individuals and groups based on social mechanisms.[7]
- Exhaustiveness: Related to Volume, Big Data becomes potentially all-encompassing of a research population, unlike with statistics, which commonly works with samples that only represent and approximate the whole—that is, the sample size is moving toward a state of N = all.[8]
- Detailed/Organic Data: Unlike Exhaustiveness, which is about sample size, organic data refers to the degree of granularity of the data within the sample; increasingly, organic data allows for a more accurate digital

https://doi.org/10.1017/S0892679415000362 Published online by Cambridge University Press

representation of physical reality in such fine detail that it approaches an organic representation of reality—metaphorically, a 1:1 map of the world.[9]

- Flexibility: Big Data encompasses *extensionality* (new dimensions can be added by adding new datasets) and *scalability* (the size of datasets can be expanded rapidly).[10]
- Virality: This factor measures how quickly data is spread and shared across networks of people (P2P) to each unique node. The time and rate of the spread of information are the determinant factors.[11] Viral diffusion differs from broadcasting in that the former, acting through a network structure, allows its individual nodes to contribute to social cascades, resulting in viral stories and posts.[12]

In sum, Big Data promises an information advantage, be it in business intelligence, state intelligence, or any other form of data gathering and analysis. At least in theory, it offers the ability to become omniscient, if not omnipotent—a promise that is tempting to any business, government, or criminal network.

New Actors and New Power Distributions

New Actors

Mainstream international relations theories of the past decades have emphasized structural explanations that privilege states and intergovernmental organizations as the primary agents of international phenomena. In these models, corporate actors as well as individuals or substate groups play a much smaller role or no role at all. These theories, however, have been challenged by the emergence of cyberspace and its capacity to empower individual action. Notably, small substate interest groups, such as those that spearheaded the Arab Spring and Occupy movements, gained traction because of their members' ability to bridge the cyber-physical gap. Big Data is adding new dimensions to these transformations as it changes the power distribution among various actors. It is crucial to understand that Big Data is now commonly viewed as the new oil—a raw material that, if refined properly, has immense value. In response, a host of new actors have arisen specializing in the collection of information from the Internet, the buying and selling of consumer data, analytics and visualization, and so on.

As individuals' digital footprints expand—through their use of credit cards, bonus/loyalty cards, cell phones, and the Internet of Things (that is, the network of everyday objects, from smart watches to firdges to cars, embedded with low-cost

https://doi.org/10.1017/S0892679415000362 Published online by Cambridge University Press

sensor technology that enables them to exchange data)—the power of these new actors only increases. Big Data collectors such as social media providers, search engines, banks, and marketing and IT companies determine which data is collected, what is stored and how, and for how long. When it comes to the quality and veracity of this data, buyers—including governments—are at the mercy of these very same data-mining companies and data brokers.

Another new type of stakeholder are Big Data utilizers, such as administrative and intelligence agencies, and companies that seek to improve their services. Utilizers reassemble different datasets and databases, (re)defining the purposes for data. In some cases, we find collectors and utilizers combined into one actor, such as Google, Microsoft, Cisco, and many smaller companies. In other cases, companies buy data sets from intermediary data brokers (such as Acxiom and Intelius) for their own analysis needs. All these actors have a great influence over the production and dissemination of knowledge and innovation. Governments are increasingly outsourcing their data collection, and sometimes even their data analysis tasks, to private actors. For example, the telecom company AT&T has reportedly been paid $10 million for storing and providing data to U.S. intelligence agencies.[13]

Since storage and processing power have become increasingly affordable, more and more small IT companies with a focus on different areas of the Big Data value chain (collection, data preparation, analysis, visualization) are emerging. Certain Big Data pools are readily accessible to anyone with a laptop or mobile device. Even if the possibility to repurpose Big Data sets remains with the Big Data utilizers, individuals can now access Big Data with varying degrees of sophistication without needing to possess the most powerful and expensive hardware. For example, with its BigQuery service, Google provides its own processing power to its customers. However, as long as most of the processing power, data gathering capabilities, and know-how in Big Data analysis remains in the hands of big companies, they will retain a distinctive competitive advantage on knowledge production and innovation vis-à-vis both individuals and states.

Individual Agency

It is well known that the Internet has revolutionized how we communicate and has empowered individuals: with the rise of online substate groups, individual agency seems to be flourishing. Big Data, on the other hand, pushes individual agency into the background. A recent case helps to illustrate this trend.

In May 2010 the website PatientsLikeMe.com—where people can share information and concerns about their diseases, exchange treatment protocols, and discuss medication recommendations—discovered a major intrusion. The Nielsen company, through its subsidiary BuzzMetrics, had scraped all data from the forum, including otherwise secret medical information. Nielsen subsequently admitted that it was mining data from 130 million blogs, eight thousand message boards, and several social media sites in order to sell it to advertisers, marketers, and pharmaceutical companies.[14] Indeed, the ordinary user of Facebook, Gmail, Yahoo, and Twitter—or even just a cell phone or credit card—has little to no choice about what data will be collected on her or him. National and regional data protection mechanisms seem to be of limited help. One is reminded of Lawrence Lessig's comment that, just as human conduct in the physical domain is regulated by laws between the citizen and the state, human conduct in the cyber domain is regulated by computer codes most often developed by corporate agencies.[15]

Correlation over Causation

One specific feature of Big Data is already progressively informing international policy and agenda setting—its privileging of correlations over causations. A frequent argument is that the fact that we are now dealing with nearly complete data sets (N = all) leads to the redundancy of theory. In other words, some have argued that correlations would replace causal models for good.[16] Such Big Data correlations already show their usefulness for policymaking. For example, the UN Global Pulse project—a Big Data-based initiative that tracks real-time developments regarding human wellbeing and vulnerabilities—found a strong correlation between Twitter conversations about the price of food and food price inflation. The Global Pulse Lab Jakarta, for example, mined Indonesian price-related Twitter data and applied a classification algorithm in order to conduct a sentiment analysis and correlate it with official food inflation statistics. If things develop in accordance with the hopes of the UN Global Pulse, in the future real-time access to macrodata analytics will help inform policymaking, allowing ad hoc adjustments to be made with a solid evidence base. Researchers are also using trend spotting and sentiment analysis to detect emergent political conflicts through web mining.[17]

One can expect that this sort of evidence-based policymaking will become more important as Big Data analysis approaches real-time. Still, while we can anticipate interesting empirical findings from Big Data-enhanced research, it is unlikely that

https://doi.org/10.1017/S0892679415000362 Published online by Cambridge University Press

it will replace theory and model building in the study of international relations. Big Data correlations sometimes do not meet the standards of scientific research, as the failure of Google Flu Trends shows.[18] Moreover, knowing that certain variables correlate does not say anything about the nature of a possible causal relationship, or whether one is even present.

Opportunities of the Big Data Age

Humanitarian and development aid agencies are dependent on reliable data for operational planning, logistics, and monitoring of their projects. In order to facilitate these processes, several platforms have been developed to provide humanitarian aid workers with open access to information, with many more on the way. This sharing of data can help facilitate aid delivery by NGOs that otherwise do not have the capability to gather intelligence on the ground themselves. For example, when a disaster strikes, humanitarian operational planning based on a rapid needs assessment should usually be ready within seventy-two hours. Using Big Data, a number of organizations have tried to help narrow this information gap.

Consider the Kenyan open-source software company Ushahidi. Ushahidi offers users the ability to upload real-time information about crises from a GPS-enabled cell phone onto a map that is freely accessible. It was used extensively to support humanitarian operations after the 2010 Haiti earthquake, and it improved the election monitoring in Kenya in 2013 (known as the Uchaguzi project), among many other examples.[19] Since most crisis-mapping tools merely consist of a website accessible with any Internet-enabled device, Ushahidi can provide aid workers with real-time intelligence in the palm of their hands. Similarly, other crisis mappers, such as the Standby Task Force and Sahanna, use overlay technology (often provided by volunteers) to project crowd-sourced information onto maps to inform humanitarian and development aid workers.

International nongovernmental organizations are also experimenting with this powerful new technology. For instance, the Humanitarian Data Exchange (HDX), a project launched by the United Nations Office for the Coordination of Humanitarian Affairs, has already assembled more than 1,500 data sets. One aggregates the number of Ebola cases and infected aid workers; another monitors water sources and opinions about water quality in Kenya; and another keeps track of total uniformed personnel of each contributing member-country by month, type (troop, police, or expert/observer), and mission.

With regard to national and international security, Big Data already plays an important role. For example, 95 percent of the police forces surveyed across the United States are actively using social media, including for investigative and intelligence purposes.[20] One of the recent advances of Big Data in national security and public safety can be seen in the area of predictive policing, which is the use of data to forecast where and at what time crimes are more likely to occur. This analysis can then be used to keep certain areas under surveillance and to preventively dispatch police units.

In October 2014, the UN Secretary-General released a report detailing how the use of technology has become an intrinsic part of decision-making, information gathering, and planning in support of the United Nations' core mandates in the areas of peace and security, development, human rights, and international law. In the words of the report: "The increasing availability of free and open-source software and open data reinforces the need for the United Nations to collaborate in the movement of big data, joined with humanitarian and social networking." For that purpose, the Secretary-General laid out a strategy to provide a common vision for the delivery of information and communications technology throughout the United Nations system, focusing on improving the organization's internal information, communication, and technology capabilities and increasingly investing in Big Data innovations.[21]

Researchers are already envisioning the role that Big Data can play in the future for UN peacekeeping and peacebuilding. John Karlsrud, for example, argues that the ongoing cyberization of conflict prevention, humanitarian action, and development, and the possibility of tracking population flows, will lead to a new generation of peacekeeping ("peacekeeping 4.0") and peacebuilding that embraces these new advancements in real-time awareness, feedback, and early-warning systems.[22]

Satellite imagery is increasingly becoming another source of Big Data analytics. Location data correlated with surveys, photos, and maps can help in uncovering war crimes. For example, in 2011 the Satellite Sentinel Programme of the Harvard Humanitarian Initiative reported finding eight mass graves in and around Kadugli, Sudan, with the help of analyzed DigitalGlobe imagery corroborated with details retrieved from UN reports and eyewitness accounts.[23]

Big Data may also be able to predict and forecast conflicts and social instabilities. For example, the U.S. Defense Department's Information Volume and Velocity program aims to harness strategic intelligence from Big Data by using

https://doi.org/10.1017/S0892679415000362 Published online by Cambridge University Press

pattern recognition to detect social instabilities in populations. And, as mentioned above, the United Nations has initiated the Global Pulse project to track real-time developments regarding human wellbeing and vulnerabilities. These kinds of programs have led some commentators to argue that Big Data might be able to help prevent future conflicts.[24]

Emerging Risks and Challenges

Big Data, however, also possesses huge potential for misuse. Humanitarian and development aid workers are at a constant risk of attack by ideologically motivated groups, but also by criminals seeking profit. Traveling with money, very little security (many aid organizations consider military escorts a violation of humanitarian principles), and expensive equipment, they are easy targets. Ushahidi and other crowd-sourced crisis mapping software provide more detailed and better structured human and signals intelligence (HUMINT and SIGINT) than criminals and armed groups could have ever hoped for just a few years ago. Crisis mappers learned this lesson when responding to the 2010 floods and food crisis in Pakistan. Pakistan-based Taliban forces threatened to attack all foreign aid workers, such as those with the World Food Programme or *Médecins Sans Frontières*, and the team operating the Pakreport.org crisis map had to rapidly change its approach to avoid allowing open-access data to be used to target humanitarians.[25]

Crisis mappers have become increasingly aware of the potential misuse of this technology. Consequently, when in 2011 the United Nations requested a group of researchers to develop a platform to map the Libya crisis, the mappers created a password-protected version of the site.[26] Big Data also reduces the individual's ability to foresee the consequences of his or her actions. This can have political consequences, as was illustrated by the case of the Russian soldier who posted geotagged photos online, indicating that, despite President Vladimir Putin's assurances, Russian soldiers were in Ukraine.

The way Big Data is used to generate insights about individuals and groups creates new types of challenges. Already, Big Data analysis on the basis of group behavior, preferences, likes/dislikes, and so on informs marketers in near real-time. At the same time, websites and web services (including Google Search) are increasingly tailored to individuals. Information gleaned from a person's prior online behavior is now employed to, say, feature certain goods available for purchase. It even determines which news items are prioritized in a search

engine or social feed. The term for this phenomenon is "ambient intelligence," and it is quietly invading all areas of technology. While personalized information can be a service, it also exposes individuals' vulnerabilities that can be exploited for the purpose of social engineering and manipulation.[27]

The rise of Big Data also presents other, fundamental, epistemic challenges. The moral and legal frameworks pioneered during the Enlightenment and codified in the postwar era are, like human rights, inherently designed around the individual actor and her specific individualistic interests, such as privacy. These norms, however, are not adequate when it comes to the privacy of groups. Many also raise concerns that this focus on groups and group behavior might lead to racial profiling, specifically in the context of predictive policing.[28]

Finally, the general public does not understand the Big Data phenomenon well enough to be particularly concerned by it, or to demand of their government specific protections from its implications. Of course, whistleblowers and investigative journalists occasionally offer glimpses into the reality of the cyber domain. But this remains insufficient to create a general public awareness of the actual digital footprint our Internet presence and cell-phone use creates. Even if the "right to be forgotten" makes sense in certain cases, applying it as an individual to one company at a time still leaves unaffected the many other data collectors and brokers that are collecting the same data and of whose activities we are not aware.

Governance of Big Data

Big Data is increasingly important in all domains of social and political life, which suggests the need for governance to curb potential abuses. In the cyber domain, actors find increasing space to steer free of limitations imposed by national legislations—a case in point is the recently dismantled website Silk Road, part of the so-called dark web, which trafficked extensively in weapons and drugs.[29] Big Data accentuates this trend of ungoverned space, as practices such as data collection and data mining are inherently global in reach. It comes as no surprise that companies and data warehouses use a variety of strategies to circumvent national and regional legislation that might limit these practices.

Take the Austrian initiative Europe-v-Facebook.org, which details Facebook's obstructive strategies in delaying the case of 25,000 European citizens trying to bring their data protection case to the European Court of Justice and other national courts.[30] For its part, Google has tried to undermine EU data protection

https://doi.org/10.1017/S0892679415000362 Published online by Cambridge University Press

measures, such as those related to the right to be forgotten. Paul Nemitz, a director in the European Commission's justice department, has even argued that Google used meetings of its advisory council in Europe as a passive-aggressive PR strategy to delegitimize the EU's data protection rules and jurisprudence.[31] National legislations are not much better equipped to tackle these challenges: a look at the *Global Data Protection Handbook* reveals that few states have adequate data protection laws or any such laws at all.[32]

Is effective international regulation, for example by an international treaty, possible? It takes just one outlier state that does not sign such a treaty on Big Data governance to jeopardize the whole endeavor. The question might be whether self-regulation, by way of a voluntary code of ethics, is a viable alternative. Such codes of conduct employ a soft form of governance that can sometimes be just as effective as laws and regulations. Not abiding by such codes can have consequences, such as public criticism, a loss of customers, and—if lawmakers and funders adopt these codes as benchmarks—the possible loss of funding and market opportunities. Of course, the creation of such a code would require the initiative of global players, civil society organizations, and academia; and these principles and decision-making heuristics would need to be open enough so as not to hamper innovation while still safeguarding against the abovementioned threats.

Conclusion

In their book *Cyberspace and International Relations*, Jan-Frederik Kremer and Benedikt Müller argue that "the global cyberspace substrate has undermined the older distinctions between international and domestic, between peace and war, between state and non-state actors, and between technology, politics, and economics."[33] I would go even further: global cyberspace, and its intensification through the ubiquitous nature of Big Data and the Internet of Things, challenges us to rethink fundamental notions of international relations and power—notions that we have taken for granted for decades.

There are many challenges ahead. Governance efforts should strive to reduce sensitive data and exploitable information from becoming open data. Furthermore, despite ongoing efforts by the European Union and other state actors to update data protection regulations—an effort that is lagging behind relentless technological innovation—the governance of nonstate actors has largely escaped national and international legislation.

When it comes to eventually developing legal frameworks, the nature of Big Data and the modus operandi of actors in the cyber domain increasingly show that the current principles guiding national and international legislation are insufficient. Groups will increasingly require their own legal protection mechanisms. In order to reduce the vulnerabilities that Big Data has imposed on society, knowledgeable stakeholders need to raise the awareness of people about the pitfalls that Big Data and their own digital footprint bring. Big Data certainly holds the promise for improving global wellbeing, and perhaps even for preventing conflicts. Nevertheless, it can also be the source of much evil. The only way to keep the misuse of Big Data in check is to create a global awareness and to use the tools that Big Data itself offers—social media and global connectedness—to enable civil society to become the public watchdog of the Big Data age.

NOTES

[1] Marc Goodman, *Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It*, ebook (New York: Knopf Doubleday Publishing Group, 2015), ch. 6.
[2] Charles J. Dunlap Jr., "The Hyper-Personalization of War: Cyber, Big Data, and the Changing Face of Conflict," *Georgetown Journal of International Affairs* 15, International Engagement on Cyber IV (2014), pp. 108–118.
[3] Rick Smolan and Jennifer Erwitt, *The Human Face of Big Data* (Sausalito, Calif.: Against All Odds Productions, 2012); Rob Kitchin, "Big Data and Human Geography: Opportunities, Challenges and Risks," *Dialogues in Human Geography* 3, no. 3 (2013), pp. 262–67; Doug Laney, "3D Data Management: Controlling Data Volume, Velocity, and Variety" (Meta Group, February 6, 2001), blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf; and Bill Vorhies, "How Many 'V's in Big Data—The Characteristics That Define Big Data," *Business Foundation Series* #2, October 31, 2013, data-magnum.com/how-many-vs-in-big-data-the-characteristics-that-define-big-data/.
[4] Ibid.
[5] Small chips attached to objects that contain electronically stored and wirelessly transferred information, e.g., for tracking and identifying parcels (functionally similar to QR codes).
[6] Richard Winter, "Big Data: Business Opportunities, Requirements, and Oracle's Approach," Executive Report, Winter Corporation, December 2011, p. 2, www.oracle.com/us/corporate/analystreports/infrastructure/winter-big-data-1438533.pdf.
[7] Andrej Zwitter, "Big Data Ethics," *Big Data & Society* 1, no. 2 (2014), p. 2; Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: Houghton Mifflin Harcourt, 2013), p. 52ff.
[8] Mayer-Schönberger and Cukier, *Big Data*, pp. 26–31.
[9] Zwitter, "Big Data Ethics," p. 2.
[10] Rob Kitchin, "Big Data, New Epistemologies and Paradigm Shifts," *Big Data & Society* 1, no. 1 (2014), p. 2.
[11] Ray Wang, "Monday's Musings: Beyond The Three V's of Big Data—Viscosity and Virality," *Forbes*, February 27, 2012.
[12] Lilian Weng, Filippo Menczer, and Yong-Yeol Ahn, "Virality Prediction and Community Structure in Social Networks," *Scientific Reports* 3, Article number: 2522 (published online August 28, 2013).
[13] Jacob Silverman, "Time to Regulate Data Brokers," *Al Jazeera America*, "Opinion" section, January 23, 2014, america.aljazeera.com/opinions/2014/1/time-to-regulatedatabrokers.html.
[14] Goodman, *Future Crimes*, ch. 4.
[15] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).
[16] Chris Anderson, "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete," *WIRED*, June 23, 2008, archive.wired.com/science/discoveries/magazine/16-07/pb_theory/.

[17] F. Johansson et al., "Detecting Emergent Conflicts through Web Mining and Visualization," Intelligence and Security Informatics Conference (EISIC), 2011 European, pp. 346–53.
[18] David Lazer et al., "The Parable of Google Flu: Traps in Big Data Analysis," *Science* 343, no. 6176 (2014), pp. 1203–205.
[19] "Ushahidi," www.ushahidi.com/, accessed April 16, 2015; and "Kenyan Elections 2013, Community Wiki—Ushahidi," wiki.ushahidi.com/display/WIKI/Uchaguzi+-+Kenyan+Elections+2013, accessed April 16, 2015.
[20] Center for Social Media, "2014 Social Media Survey Results," Annual Survey (Alexandria, Va.: International Association of Chiefs of Police, Fall 2014), www.iacpsocialmedia.org/Resources/Publications/2014SurveyResults.aspx.
[21] UN Secretary-General, "Information and Communications Technology in the United Nations," Report of the Secretary-General to the General Assembly, October 10, 2014, UN document A/69/517, para. 40.
[22] John Karlsrud, "Peacekeeping 4.0: Harnessing the Potential of Big Data, Social Media, and Cyber Technologies," in Jan-Frederik Kremer and Benedikt Müller, eds., *Cyberspace and International Relations: Theory, Prospects and Challenges*, 2014 edition (Heidelberg, Ger.: Springer, 2013), pp. 141–60.
[23] Satellite Sentinel Project, "Evidence of Burial of Human Remains in Kadugli, South Kordofan," Special Report, Harvard Humanitarian Initiative, August 24, 2011, hhi.harvard.edu/publications/special-report-evidence-burial-human-remains-kadugli-south-kordofan.
[24] Sheldon Himelfarb, "Can Big Data Stop Wars Before They Happen?" *Foreign Policy*, April 25, 2014, foreignpolicy.com/2014/04/25/can-big-data-stop-wars-before-they-happen/.
[25] Rasool Dawar (*Associated Press*), "Taliban Threatens Foreign Aid Workers," *Washington Times* online, August 26, 2010, www.washingtontimes.com/news/2010/aug/26/taliban-threatens-foreign-aid-workers/.
[26] Marc Parry, "Academics Join Relief Efforts Around the World as Crisis Mappers," *Chronicle of Higher Education*, March 27, 2011, chronicle.com/article/Academics-Join-Relief-Efforts/126912/.
[27] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Cheltenham, U.K.: Edward Elgar Pub, 2015), p. 90.
[28] John J. Reilly Center of the University of Notre Dame, "Predictive Policing," reilly.nd.edu/outreach/emerging-ethical-dilemmas-and-policy-issues-in-science-and-technology-2014/predictive-policing/.
[29] I.e., a website that cannot be indexed by search engines and to which one only has access through identity-cloaking protocols such as *Tor*.
[30] "Europe-v-Facebook.org," www.europe-v-facebook.org, accessed August 28, 2015.
[31] *Reuters*, "Google Accused of 'Passive-Aggressiveness' over EU Right to Be Forgotten," *Telegraph*, "Technology" section, November 5, 2014, www.telegraph.co.uk/technology/google/11210836/Google-accused-of-passive-aggressiveness-over-EU-right-to-be-forgotten.html.
[32] "Global Data Protection Handbook," dlapiperdataprotection.com/#handbook/world-map-section/c1_AR/c2_EG, accessed April 16, 2015.
[33] Jan-Frederik Kremer and Benedikt Müller, eds., *Cyberspace and International Relations: Theory, Prospects and Challenges*, 2014 edition (Heidelberg, Ger.: Springer, 2013), p. vii.