Ebola: A Big Data Disaster

Privacy, Property, and the Law of Disaster Experimentation

Sean Martin McDonald

CIS Papers 2016.01

Ebola: A Big Data Disaster

Privacy, Property, and the Law of Disaster Experimentation

CIS Papers 2016.01, March 2016

http://cis-india.org/papers/ebola-a-big-data-disaster

CIS Papers

The CIS Papers series publishes open access monographs and discussion pieces that critically contribute to the debates on digital technologies and society. It includes publication of new findings and observations, of work-in-progress, and of critical review of existing materials. These may be authored by researchers at or affiliated to CIS, by external researchers and practitioners, or by a group of discussants. CIS offers editorial support to the selected monographs and discussion pieces. The views expressed, however, are of the authors' alone.

Author

Sean Martin McDonald, Occam Technologies, Inc., 1110 Vermont Ave, Suite 500, Washington, DC 20005, United States of America. Website: http://www.frontlinesms.com/.

Publisher

The Centre for Internet and Society, Bengaluru and Delhi, India. Website: http://cis-india.org/.

Copyright and License

Layout and Typography

Layout is designed by Sumandro Chattapadhyay. Text is set in Fira Mono and Sans. Details: https://github.com/mozilla/Fira.

Grant Details and Disclaimer

This paper was made possible by a grant from the Media Democracy Fund. All activities by Occam Technologies, Inc. were and are consistent under the Internal Revenue Code Sections 501(c)(3) and 509(a)(1), (2), or (3). If any lobbying was conducted by Occam Technologies, Inc. (whether or not discussed in the report), Occam Technologies, Inc. complied with the applicable limits of Internal Revenue Code Sections 501(c)(3) and/or 501(h) and 4911. Occam Technologies warrants that it is in full compliance with its Grant Agreement with the New Venture Fund, dated June 29, 2015, and, that, if the grant was subject to any restrictions, all such restrictions were observed.

Table of Contents

Preface

This study titled “Ebola: A Big Data Disaster” by Sean Martin McDonald, undertaken with support from the Open Society Foundation, Ford Foundation, and Media Democracy Fund, explores the use of Big Data in the form of Call Detail Record (CDR) data in humanitarian crisis. It discusses the challenges of digital humanitarian coordination in health emergencies like the Ebola outbreak in West Africa, and the marked tension in the debate around experimentation with humanitarian technologies and the impact on privacy. McDonald’s research focuses on the two primary legal and human rights frameworks, privacy and property, to question the impact of unregulated use of CDR’s on human rights. It also highlights how the diffusion of data science to the realm of international development constitutes a genuine opportunity to bring powerful new tools to fight crisis and emergencies.

Analysing the risks of using CDRs to perform migration analysis and contact tracing without user consent, as well as the application of big data to disease surveillance is an important entry point into the debate around use of Big Data for development and humanitarian aid. The paper also raises crucial questions of legal significance about the access to information, the limitation of data sharing, and the concept of proportionality in privacy invasion in the public good. These issues hold great relevance in today's time where big data and its emerging role for development, involving its actual and potential uses as well as harms is under consideration across the world.

The paper highlights the absence of a dialogue around the significant legal risks posed by the collection, use, and international transfer of personally identifiable data and humanitarian information, and the grey areas around assumptions of public good. The paper calls for a critical discussion around the experimental nature of data modelling in emergency response due to mismanagement of information has been largely emphasized to protect the contours of human rights.

This study offers an important perspective for us at the Centre for Internet and Society, and our works on Privacy, Big Data, and Big Data for Development, and very productively articulates the risks of adopting solutions to issues important for development without taking into consideration legal implications and the larger impact on human rights. We look forward to continue to critically engage with issues raised by Big Data in the context of human rights and sustainable development, and bring together diverse perspectives on these issues.

Elonnai Hickok

Policy Director, the Centre for Internet and Society

Executive Summary

Digitizing disaster response invites the problems of digital systems into the most fragile and vulnerable environments in the world. Troublingly, it is often humanitarian organizations that lead the charge, underestimating the practical and legal implications of digitizing these systems, from data security to operational coordination to the fairness of algorithms. In addition to their own digital transformations, many humanitarian organizations actively encourage governments, charitable foundations, technology companies, and mobile networks to share data in ways that are illegal without user consent or the invocation of governmental emergency powers. The governance of emergency powers over digital systems remain poorly defined and badly regulated, and lack the basic due process checks and balances that exist for nearly every other kind of government emergency authority. The humanitarian community knows that it does not have the technological, legal, or institutional checks necessary to fairly or fully realize the promise of digital systems. That knowledge, however, hasn't prevented many of the world's most important and trusted institutions from taking irresponsible, at best, and illegal, at worst, risks with some of the world's most sensitive data.

The most prominent of these risks is the growing call for mobile network operators – the companies that provide mobile phone and data services – databases, which usually contain a significant amount of personal information. According to the most frequently cited expert for justifying the release of mobile phone records, we simply don't have a sufficient understanding of how to apply these records to social services systems—even less so in fragile contexts. The humanitarian community lacks the data modeling, professional technology implementation standards, and the enforcement capacity to protect, or even define, the public's interest. Even in places where there are regulatory institutions to fill the gap, emergency contexts often cause disruption or suspension of the safeguarding processes required to protect human rights. Without these processes – or any other form of public oversight – digitizing humanitarian systems can add layers of opacity to the already complex data models, implementation approaches, or intended outcomes of the response, further crippling tenuous public trust and good governance.

Where this leaves us is a world where the stretching and violation of national, regional, and international human rights and data protection laws has become the norm, for a benefit that practically eludes definition, if it even exists. Despite that, many governments, businesses, and international organizations are routinely given access to mobile network operator data – Call Detail Records (CDRs), containing some of the most personal, re-identifiable data that people produce today. Humanitarian, academic, and journalistic calls for the release of CDRs gain the most traction in emergencies, contributing to a norm that actively disregards individual rights and consent. These practices not only put individuals at risk of harm, but as digital jurisprudence continues to come

into its own, they will put many of the world's best—and best-intentioned—international organizations at risk of onerous lawsuits.

There is no more visible or apt example of this than the West African Ebola outbreak, which became a global health scare in 2014. This case study focuses on Liberia to illustrate (1) the challenges of digital humanitarian coordination during the Ebola outbreak; (2) the nascent state of mobile data modeling's utility during complex emergencies; (3) the marked tension in the debate around experimentation with humanitarian technologies; (4) the laws that govern mobile network data and individual privacy; and (5) the institutions where victims of these data breaches could bring legal action.

In 2014, a small outbreak of Ebola in West Africa grew into a global health crisis. Over the ensuing 18 months, Ebola infected almost 30,000 people and killed over 11,000. Although a large number of factors led to the spread of the disease, the early stages were characterized by rumor, misinformation, and a deep distrust of the institutions responding to the disaster. By the time the international community mobilized, the epidemic had been metastasizing for nine months, and required significantly more investment than initially anticipated. International health and humanitarian response agencies made apocalyptic predictions about the epidemic, sparking panic and uncertainty. A new wave of foundations, donors, and organizations took an interest in the response, leading to a surge in people, resources, and operational chaos. That chaos fed a growing narrative that the problem in the response effort was a lack of good information technology and, more specifically, data.

The focus on technology catalyzed the introduction and adaptation of an enormous number of information systems, mostly through ad hoc imposition or adoption. Over the course of the epidemic, the operational infrastructure of the response involved more than 50 independent technology tools. One group catalogued more than 300 separate initiatives to engage the public, a small minority of which had any operational role or capacity. In addition to the usual challenges of coordinating a disaster response, the Ebola outbreak highlighted the difficulty of syncing information infrastructure with operations.

As the epidemic began to peak, a group of academics and international development actors began to call for the use of aggregated location data from mobile phone networks in order to facilitate the response effort. These calls suggested that with real-time location data taken from mobile phone networks, responders could at least target response efforts and may be able to perform a process called contact tracing. Contact tracing historically refers to manual efforts to track the spread of contact-based diseases, like Ebola. The Ebola response included hundreds of contact tracers, who personally interviewed everyone infected and everyone they were exposed to. The theory was that with the ability to track aggregate movement patterns, the response movement could create a predictive model for the spread of the disease. A significant number of professional, donor and think tank organizations invested in various aspects of supporting the release of call detail records

(CDRs), and nearly every affected country did – except for Liberia. Despite having the highest death toll of any country that experienced the Ebola epidemic, Liberia never compelled the release of CDRs, in part, due to concern about their ability to manage and enforce the necessary limitations.

Mobile phone records, however, are one of the most personally identifying and regulated data sources in the world, raising significant privacy and property law questions. Nearly all of the discussion of the use of CDRs in the Ebola response referenced privacy as a concern, but didn't interrogate the value of real-time data or the applicable legal frameworks. The vast majority of the examples given to justify the use of CDRs were vector-borne disease, meaning that probabilistic models bear out. However, Ebola is not a vector-borne disease, meaning that the same probabilities aren't a useful indicator of transmission. At present, even the organizations designing and building the data models aimed at contact tracing urge more experimentation and nuance in the application of big data to disease surveillance. The privacy of people's data within CDRs, let alone CDRs themselves, is nearly impossible to guarantee, even when anonymized – individuals can often be re-identified and records require correlation with personally identifying information in order to be a useful predictor of a contact-based disease. In this way, using CDRs to contact trace Ebola provides a stark trade-off between the potential of an experimental process and the very tangible threat to user rights.

This analysis focuses on the two primary legal and human rights frameworks triggered by the release of CDRs: privacy and property rights. The right to privacy in Liberia emanates from the Constitution, and is subsequently defined in the Economic Community of West African States (ECOWAS) Supplementary Act and the Liberian Telecommunications Act of 2007. These laws, taken together, form a broad protection for the privacy of mobile data – requiring user consent or a governmental invocation of emergency powers in order to compel their release. Even in an emergency, the available law does not protect mobile network operators or the Government of Liberia, let alone third party organizations, from a civil or human rights lawsuit. The Constitution of Liberia grants similarly broad protections for private property, though it also contains provisions for expropriation. Although there are additional emergency powers granted to the President through the Public Health Law, all property seizure requires elements of due process and fair compensation. The presence of these laws takes the legal risk of using CDRs without user consent out of the hypothetical, and offers significant causes of action against a wide range of parties.

Despite the available causes of legal action, constructing a useful case and selecting an appropriate venue for each component claim is extremely complex – and likely to be very expensive. Private commercial dispute resolution and industry regulation offer the best likelihood of reforming practice, though international human rights courts have the most aligned incentives, capacity, and mandate to provide legally binding remedies. Even with these mechanisms, many of the core concepts – such as the legal liability and limitation of data sharing, the concept of proportionality in privacy invasion in the public good, and an evaluative framework for disaster

data models – will take years to evolve into legal significance. These practices, though, already have significance, and deserve legal attention and definition to protect basic human rights. No matter whether such efforts are successful, there is no question that Ebola will not be big data's last disaster.

Foreword

In June of 2015, South Korea was struck by an outbreak of Middle East Respiratory Syndrome (MERS), killing 36 people (out of 186 infected). During their response, the Government of South Korea did something truly unprecedented – it used citizens' personal information, taken from mobile phone company databases, to impose quarantine on more than 17,000 people. These quarantines were not always based on direct evidence of contact or infection - they were imposed based on probabilities of infection.

The Government of South Korea used algorithms to pre-emptively restrict the movement of thousands of people without any direct evidence of infection, for a disease that is relatively difficult to transmit. The outbreak and the quarantines were devastating to the economy, reducing tourism by 40 percent and causing the Government to deploy $9 billion in relief.

Although most citizens in South Korea are reportedly willing to consent to this use of their data, many suggest that public consent is uninformed and stoked by anxiety – largely due to the opacity of the Government's response effort. More concerning, the Ministry of Health has made it clear that they don't need public consent to obtain personal information or to impose quarantine for "the public good."

What we don't know is whether that seizure of information resulted in a public good. Quite the opposite, there is limited evidence to suggest that migration or location information is a useful predictor of the spread of MERS at all. There is even less evidence to prove that the seizure of data was necessary to gather location information or that the imposition of quarantine helped contain the virus. There has been no public presentation about whether or how mobile data information was actually used – or what the effect of that use was. There is ample evidence to show that it significantly damaged the economy of South Korea and the freedom of South Koreans. Without more transparency, it's simply impossible to know whether Government of South Korea acted necessarily, effectively, or proportionally to contain the MERS outbreak.

Fundamentally, this type of government action amounts to the exercise of a new type of emergency powers, built on an undisclosed algorithm. Large-scale quarantine is—other than civil war, martial law, and internment camps—the most severe restriction of freedom that a government makes against its own people with the implicit threat of force. And it is the only one that takes place without a violent, causal event. Collecting and seizing personal mobile phone records is the most egregious violation of individual's digital human rights– let alone as a commercial or national security asset. In almost every democracy, the assertion of emergency powers are subject to due process analyses, at least by the legislature – if not the executive branch or security apparatus. There's no question that emergency situations change the cost-benefit analysis, but they do not justify untested or inapplicable methods, nor the large-scale restriction of a people's freedom in

peacetime without just cause. The growing emergence of this new brand of emergency powers, unchecked due process, is why I decided to write this paper. That these powers are largely being outsourced to international organizations without the institutional capacity, processes, regulation, standards, infrastructure, or appropriate risk frameworks, is why we should all be concerned.

The demands of the humanitarian community for increasingly large amounts of otherwise legally impossible to obtain data are growing with every disaster. These requests are not only increasingly audacious, they're also increasingly vague – and, unlike the South Korean case, driven almost entirely by international donors and responders. Responsible actors acknowledge the need for policies and privacy frameworks, but they ignore the existing laws—international treaties, commercial regulation, and national data protection laws—that explicitly prohibit these requests. Worse, the organizations charged with building institutions and mitigating harm in the world's most fragile environments are relying on the weakness of the same institutions to grant these requests. Just as there has been in nearly every other industry, the humanitarian industry is experiencing its digital gold rush – and a whole host of new and established agencies alike are using every tool at their disposal to gain an advantage.

The best example of this dynamic is the recent Ebola epidemic in West Africa. This outbreak was called the "worst health crisis in many, many years," by seasoned disaster responders – and catalyzed a large number of international attention in an effort to contain the virus. The epidemic response introduced an unprecedented amount of information technology – and a commensurate amount of complexity. Information technology and mobile data records became two of the highest-profile elements of the epidemic. In both Korea and West Africa, the focus on data collection, seizure, and sharing ignores the legal and practical implications involved.

Within the Ebola outbreak, Liberia was the tipping point, where lack of faith in institutions transformed the outbreak from a containable health emergency to a global pandemic. Despite the enormous death toll and operational chaos, Liberia uniquely refused to share mobile network data with international organizations, despite repeated requests. Liberia is also a member of ECOWAS, which has some of the most sophisticated, if unimplemented, data protection law in the world. Liberia is an ideal case study to demonstrate the diversity and depth of potential international, regional, and local legal risks in the practices that growingly characterize digital humanitarian interventions.

This case study is based on a combination of desk and in-country research. The desk research comprised an extensive literature review of news, operational reports from the Government of Liberia, international organizations, and media coverage. The researcher conducted in-person interviews with more than 20 key stakeholders that were directly involved in managing information systems in Liberia during the Ebola epidemic. The researcher has direct experience deploying technology in humanitarian disasters all over the world, including during the Ebola epidemic.

Chapter 1: The Epidemiology of Uncertainty

The Ebola epidemic was the first pandemic of the Information Age and it publicly demonstrated the global interdependence of health systems. The West African outbreak was also one of the first global emergencies where humanitarian organizations blamed a lack of access to mobile network data as a primary driver of its death toll. For the first time, people all over the world watched as fragile West African health systems struggled, and ultimately failed, to control an outbreak. Ebola spread beyond West Africa, to the United States and Spain. Although those nations effectively contained the virus, the epidemic tangibly proved that every fragile healthcare system poses a threat to global health. The spread of the disease and its high regional death toll aren't just an indictment of West African health systems, they are also a damning indicator of international community's reaction. There are many political, economic, and logistically complex reasons for the delay in response – but by far the most publicly cited reason is information. Health and governmental institutions at every level failed to manage the information about the Ebola virus and its spread, causing massive delays, inefficiencies, and panic.

In December of 2013, a single case of the Ebola virus killed a young girl in Guinea. Unlike the 24 previous incidents of Ebola in Sub-Saharan Africa, this outbreak spread to the urban centers of West Africa, growing through a combination of mismanagement and misinformation.[1] The outbreak became epidemic that has killed more than 11,000 people in Liberia, Guinea, and Sierra Leone - and isn't over.

Within Guinea, Sierra Leone, and, particularly, Liberia, the spread of Ebola significantly damaged the already tenuous trust between the government, the media, and the public. Many governments released conflicting denials, reports, and warnings about the spread of Ebola, complicating what were already very weak relationships. Contradictory reports further damaged the public's remaining faith in institutional narratives, enabling rumor to take the place of fact.

In Liberia, journalists have a primarily antagonistic relationship with the government, meaning that they often amplified suspicion, by advancing their own accounts of events or Ebola itself. The absence of a legitimate, unified voice was felt throughout the social and political ranks. Some believed that Ebola wasn't real at all. Others believed that Ebola was engineered by the Liberian Government to attract international funding. Almost two years into the epidemic, some still wonder aloud whether it was a plot by the American military to chase terrorist cells in the region. An International Alert study found that 81% of Liberians were angry with the Government of Liberia for their handling of the outbreak.[2] Regardless of the specific rumor, chaos and anger were uniform.

1 Epstein, Helen. "Ebola in Liberia: An Epidemic of Rumors." The New York Review of Books (online) 18 December 2014: http://www.nybooks.com/articles/2014/12/18/ebola-liberia-epidemic-rumors/.

2 Mukpo, Ashoka. "Surviving Ebola: Public perceptions of Governance and the outbreak response in Liberia." International Alert 30 June 2015: http://reliefweb.int/report/liberia/surviving-ebola-public-perceptions-governance-and-outbreak-response-liberia.

Even without confusion, the health systems in the affected countries didn't have the facilities, capacity, or resources to contain a disease like Ebola. Ebola has a gestation period of 21 days, meaning an infected person can wait weeks before experiencing a symptom. The unique characteristics of the virus required affected health systems to build parallel infrastructure to track, treat, and bury patients. Each unit had to be capable of identifying, holding, testing, and treating patients – and everyone they'd come into contact with after exhibiting symptoms – for weeks to be sure they weren't infected. Even committing every major healthcare facility and ambulance to the response, Liberia did not have the dispatch or response resources to manage reports of Ebola, let alone the usual health needs of the country.

At the peak of the epidemic, the estimated cost of building and maintaining an Ebola Treatment Unit were $170,000 and $1m per month per facility, respectively.[3] By July of 2014, before the international community deployed and the peak of the epidemic, the Liberian response already had a $15m dollar shortfall.[4] The affected countries simply did not have the means to independently isolate and contain the Ebola epidemic. The financial and practical costs of building a parallel health system meant that the government was forced to turn to international organizations for assistance.

The international humanitarian and health systems, however, responses faced a different set of challenges, leading to significant tension with the national governments of affected countries. The national governments were afraid of capital flight if the international business community learned about the epidemic, whereas international responders were dependent on public concern to motivate resource donations and political pressure. The World Health Organization, for example, is not equipped for emergency response – it's wholly dependent on donations for core funding to respond to public health crises.[5] As a result, the international health community was slow to mobilize. The WHO didn't declare the Ebola epidemic a Public Health Emergency of International Concern (PHEIC) until August 8, 2014.[6] That was 9 months after the outbreak began in Guinea, 6 months after receiving warnings from their internal regional teams, and 4 days before the death toll reached 1,000.[7] More than a month later, the UN established the United Nations Mission for Emergency Ebola Response (UNMEER), an independent responder that acted independently of the humanitarian and health response communities.[8] The delay in official response was more than a bureaucratic disaster - it allowed both the epidemic and rumors that surrounded it to grow. "They

3 "Much worse to come." The Economist (online) 18 October 2014: http://www.economist.com/news/international/21625813-ebola-epidemic-west-africa-poses-catastrophic-threat-region-and-could-yet.

4 "Liberia Operational Plan for Accelerated Response to the Re-Occurrence of the Ebola Epidemic." Government of Liberia, Ministry of Health and Social Welfare. July- December 2014: http://www.who.int/csr/disease/ebola/evd-outbreak-response-plan-west-africa-2014-annex3.pdf.

5 "Report of the Ebola Interim Assessment Panel" World Health Organization, pg. 12. 7 July 2015: http://www.who.int/csr/resources/publications/ebola/ebola-panel-report/en/.

6 Ibid.

7 Davis, Rebecca. "Ebola epidemic 2014: timeline." The Guardian (online) 15 October 2014: http://www.theguardian.com/world/2014/oct/15/ebola-epidemic-2014-timeline.

8 "Report of the Ebola Interim Assessment Panel" World Health Organization, pg. 24. 7 July 2015: http://www.who.int/csr/resources/publications/ebola/ebola-panel-report/en/.

came in very late," said Tolbert Nyenswah, Liberia's Assistant Minister of Health, "and because they came in very late, we are suffering this today."[9]

When the international community did deploy, it got the world's attention – but not in the way that it intended. Almost immediately after declaring an emergency, the WHO and the Centers for Disease Control and Prevention (CDC) made nearly apocalyptic projections about the scale and mortality of the epidemic – adding the telling caveat "without more intervention." The WHO projected that Ebola's mortality rate could reach 90 percent in August of 2014, when mortality rates ranged between 42 and 74 percent.[10] In September of 2014, the CDC projected that the epidemic could hit between 550,000 and 1.4m cases by January of 2015.[11] These projections were overstated - the total number of reported cases is under 30,000 and the mortality rate was closer to 70 percent.[12] The motivation for these projections is the subject of a lot of speculation, but their accuracy leave less to debate.

The WHO and CDC's statements came at a critical time during the response, and ultimately traded public faith for financial support. The international community's messaging successfully motivated the commitment of billions of dollars in support – but it also incited panic in the public and responder communities. As in the affected countries, the lack of a credible voice led to the politicization of the response effort - causing travel restrictions, protectionism, and significant delays. The international donor community simultaneously committed hundreds of millions of dollars and refused to supply doctors.[13] By September of 2014, the concerns about responder capacity became so severe that Médecins Sans Frontières (MSF) – a traditionally neutral humanitarian organization – called for military intervention.[14] In October of 2014, 10 months into the epidemic, there were only two international non-profit organizations supporting treatment efforts – and they struggled to recruit qualified volunteers.[15] The international community was successful in compelling public resources to combat Ebola, but in doing so, had to foster a narrative of chaos, fear, and uncertainty.

The dependence of international health and humanitarian response on volunteer donations engenders fierce competition among responders, creating an ongoing incentive to sensationalize

9 York, Geoffrey "Only a few aid agencies willing to help fight Ebola in Africa." The Globe and Mail (online) 3 October 2014: http://www.theglobeandmail.com/news/world/aid-agencies-fail-to-mobilize-ebola-resources/article20930983/.

10 Kelland, Kate "Ebola mortality rate expected to rise as outbreak runs its deadly course." Reuters (online) 5 August 2014: http://www.reuters.com/article/2014/08/05/us-health-ebola-mortality-idUSKBN0G526M20140805.

11 Glennerster, Rachel; M'Cleod, Herbert, and Suri, Tavneet, "How Bad Data Fed the Ebola Epidemic." The New York Times Op-Ed (online) 30 January 2015: http://www.nytimes.com/2015/01/31/opinion/how-bad-data-fed-the-ebola-epidemic.html?_r=2.

12 "Ebola: Mapping the Outbreak" BBC News Africa (online) 19 June 2015: http://www.bbc.co.uk/news/world-africa-28755033.

13 "Much worse to come." The Economist (online) 18 October 2014: http://www.economist.com/news/international/21625813-ebola-epidemic-west-africa-poses-catastrophic-threat-region-and-could-yet.

14 MSF called for the United Nations members to deploy biohazard containment teams, which are typically military units trained to respond to biological and chemical weapons. Pérache, André Heller. "'To put out this fire, we must run into the burning building': a review of MSF's call for biological containment teams in West Africa." Humanitarian Exchange Magazine, Issue 64 June 2015: http://www.odihpn.org/humanitarian-exchange-magazine/issue-64/to-put-out-this-fire-we-must-run-into-the-burning-building-a-review-of-msfs-call-for-biological-containment-teams-in-west-africa.

15 York, Geoffrey "Only a few aid agencies willing to help fight Ebola in Africa." The Globe and Mail (online) 3 October 2014: http://www.theglobeandmail.com/news/world/aid-agencies-fail-to-mobilize-ebola-resources/article20930983/.

disasters (even the word ‘disaster’ is itself sensational). In an age where information and resources move globally, with little regard for borders, humanitarian organizations have been lax to apply their principles to the newly compounded effects of their communications and response efforts. The Ebola epidemic may have been one of the most successful mobilizations of international donations in history, but that success likely came at the expense of institutional trust, operational coordination, and the lives of victims.

Chapter 2: A Digitizing Disaster

Operational chaos is par for the course in disaster – and the Ebola epidemic is no exception, but it is among the first to so visibly struggle with digitization. Nearly every after-action review of the response points to the lack of structure or foundation to coordinate response during a global pandemic. What was unique to the emerging narrative of the Ebola epidemic, both during and after the height of the crisis, was the degree to which it focuses on health information systems and data.[16] Media coverage and international organizations spent significant resources creating a market for interoperability in health information technologies and advocating for the public and humanitarian use of mobile network data. The funding, coverage, and growingly digital practices of humanitarian agencies catalyzed a rapid proliferation of digital interventions in Liberia. These interventions were rarely coordinated, often unrelated to the response effort, and caused more confusion than benefit. The digitization of the Ebola response compounded the challenges of humanitarian response with the challenges of information system harmonization, without solving the significant legal, financial, and practical risks involved.

Altering control of and access to information fundamentally alters the underlying power relationships around them. Publicly releasing operational health system information may undermine the ability of national governments or international coordination bodies to compel and coordinate response efforts. Similarly, compelling mobile network operators to provide real-time access to their data infrastructure, even with privacy protections in place, without user consent extra-legally surrenders some of the most personal data individuals generate. The assumption that open and interoperable data will lead to better health response is untested, as is the assumption that mobile network data records measurably improve health system response efforts. There are fewer questions about whether access to large datasets that are typically subject to commercial, privacy, and governmental restriction, is valuable. Opening health information systems and mobile network data implicitly reduces dependence and decentralizes response capacity – which may improve outcomes, but it may also substantially complicate the already significant challenges involved in creating a coordinated, cohesive response.

Ad Hoc Hierarchy

Health systems, even in emergency, are hierarchically organized – as a matter of sovereignty and, ideally, practicality. The structure of health information systems typically map to those hierarchies

16 Although coverage varied, technology played prominently as a theme in Ebola coverage – ranging from big data analysis platforms to mobile phones. Coverage came from nearly every globally influential publication, including the Guardian, New York Times, the Economist, Der Spiegel, Al Jazeera, and many others. Coverage also extended to academic and industry publications. This research was not able to provide a comprehensive coverage assessment, but Google returns 25,200,000 results for "Ebola and Technology," – whereas "Ebola and 'West Africa,'" returns 12,500,00 results. Within that, Google returns 485,000 results for "Ebola and 'mobile phone,'" and 437,000 results for "Ebola and "big data." This is far from scientific, but lends to the assertion that there was a significant amount of globally influential coverage.

with varying indicator definition, data format, and reporting structure standards. The health system in Liberia was no exception, though it primarily used paper records – transported at regular intervals to the Ministry of Health (MoH) for aggregation, digitization, and analysis. In some cases, paper records were digitized for aggregated reporting to the MoH – but rarely in real-time and never toward the level of awareness required during an active epidemic.

When the international community came in, it made digitizing health information a priority – sometimes consciously, sometimes as a logistical afterthought. Regardless of intent, digitization was initially piecemeal, which added another logistical challenge between the people and systems trying to build a systemic response. Although there were significant problems in building a functional information reporting and response system, the vast majority of the challenges faced by responders were organizational, operational, and political.

Organizational Digitization, Inter-Organizational Disconnection

Each organization within the response effort had their own digital infrastructure, almost all of which were proprietary and tailored to their own use case. It's important to note the distinction between individual habit and technological interoperability – many of the systems used to respond to the Ebola epidemic were technologically capable of being integrated with other systems. However, the disaster response organizations very rarely took the time to synchronize the definitions and formats of information collected, create or enforce data licensing relationships, or even understand partner systems. Even the ad hoc responder coalitions that initially shared data and technology systems, shrunk and came apart during the disaster.[17]

> People just wanted to contribute in a way that could make impact and learning new tools would delay that. Collaboration is time consuming... they didn't want to express any kind of hindrance on what could be implemented in a short time period. Overall, I just sensed that a lot of these people wanted to own their data, they wanted to have some kind of information power.[18]

One of the emergent problems of modern disaster response is that humanitarian responders focus on direct impact – meaning that they discount the value and importance of building functional communication standards and coordination frameworks. The result is that responders neither have the time, nor the inclination, to learn new technological systems once they're deployed. The natural resistance to learning new systems coupled with the exigency of the epidemic adds informational disconnect to the typical coordination challenges during disaster.

17 There were a significant number of alternative health information systems created for small coalitions of responders. The International Rescue Committee formed one such coalition – and database system, for its own use, in collaboration with Global Communities, the iLab, Medical Team International, and Action Against Hunger. According to one of their leads, they began by using the MoH's system – DHIS 2 – but felt as though the interface and platform didn't meet their needs, nor did having to interface with the Government as intermediaries. Interview. Augustine Kornyon, Data Coordinator for the International Rescue Committee. 24 September 2015.

18 Interview. Carter Draper, Information Coordinator with iLab Liberia. 21 September 2015.

The financial (and personal) incentives for disaster response organizations favor those that are able to prove unique impact in a short period of time, which is rarely measured through collaboration or collective impact. As Carter Draper, who helped coordinate several information systems for response organizations through the iLab in Liberia, said; "[i]f it wasn't part of their mandate, they weren't going to do it – they could barely do what their mandate was."[19] Inter-organizational data sharing is rarely a contractual requirement for response organizations, and therefore not measured – meaning that it not only causes operational drag, it actively erodes competitive advantage. It is practically easier and financially beneficial for humanitarian organizations to develop their own information systems, instead of focusing on building functional communication sharing.

Operational Context and Complexity

The information chaos, like the operational chaos, was pronounced and became a defining characteristic of the response effort. Prior to the epidemic, the MoH managed data through three independent units: (1) the Health Management Information System, which generated data through the healthcare system; (2) the Research Unit, which provided analysis, evidence, and structure; and (3) the Monitoring and Evaluation Department, which tracked trends and the overall effectiveness of the healthcare system.[20] Below the level of the MoH, there are subsystems that vary by geography (counties and districts), facility (emergency dispatch, triage unit, lab, treatment center, hospital), and health system function (investigation, holding, testing, treatment). Each component system functioned independently, producing its own records and periodically reporting to the MoH. Ultimately, these systems produce an enormous amount of information – they record every point of patient contact – they just do it in paper forms, limiting its utility and usability.

When Ebola struck, the MoH and, eventually, international organizations built an almost entirely parallel ad hoc health system designed to identify, separate, and treat the virus. Each ad hoc component brought its own ad hoc information system. "Everything around Ebola – the reporting, data collection, and information sharing mechanisms were all ad hoc structures that we manage," said Luke Bawo, the Head of the Information Management Systems.[21] Even his position, as central coordinator of information systems, was created during the Ebola outbreak, based on the need to integrate existing information management infrastructure and those of international actors into a single operational framework. That job is no small feat - there were more than 50 separate technology systems introduced during the response effort alone.[22] Bawo is responsible for synchronizing data consumers and producers of data, operating from different baselines and largely relying on Liberian agencies to ensure data quality, availability, and coordination.[23]

19 Interview. Carter Draper, Information Coordinator with iLab Liberia. 21 September 2015.
20 Interview, Luke Bawo, Head of the Information Management System, Ministry of Health. 26 September 2015.
21 Interview, Luke Bawo, Head of Information Management Systems, Ministry of Health. 26 September 2015.
22 FORTHCOMING. "Regional, Real-Time Data Infrastructure for Ebola Response." Gobee Group July 2015, pg 52.
23 Interview. Thomas Davis, Director of Geographic Information Services, Liberian Information Service. 22 September 2015.

Data, Sovereignty, and the Politics of Control

Every new health information system created or introduced during the response also has a de facto responsibility to integrate with the MoH's reporting requirements, data definitions, and, most importantly, operational infrastructure. That responsibility emanates from the Government's sovereign responsibility for the health of its people. Though that concept is broadly acknowledged, it doesn't have a clear operational or implementation framework. That ambiguity means that the authority to compel reporting inputs and approve requests for information is almost as ad hoc as the rest of the operational response infrastructure. That creates the space for international organizations to push back against reporting requirements to the Government of Liberia, which they did.[24] Nearly everyone interviewed suggested that international organizations were more focused on consuming information than creating a two-way reporting relationship with the MoH. This became a significant source of tension – some responders shared information within their own organizational hierarchies more quickly and regularly than they did with the MoH. In at least one instance, this resulted in new Ebola deaths being reported by a responder's headquarters before the MoH knew about it – causing a political backlash.

On the other side, the Government was under-resourced to manage its own response efforts, which also manifested in information management processes. Many of the private and international organizations describe functional difficulties using the MoH's system, and procedural challenges in coordinating with the Government.[25] The sheer magnitude of the response, exigency of the epidemic, and volume of chaos, made it nearly impossible to manage communication in real-time. The technological syncing of data reporting systems is a complicated and unfinished technical task in the best of circumstances – but the underlying information relationships during the Ebola response were a proxy for larger political negotiations about roles, authority, and resources.

The Government of Liberia wanted to be the single authoritative source of information on the epidemic. Although there weren't any publicly documented objections, the response effort wasn't coordinated enough to make a command-and-control approach practical. The Government of Liberia uses a primarily form-based application process to manage information requests. The applications are fairly lightweight, requiring date, organization, and purpose – but not much else. There are variations based on type of information and logistics (including things like desired data format) for processed data. Even with established processes, many of the implementing offices were either under-resourced or outright shut down – leading some organizations to seek authority and guidance from international data ethics institutions.[26] There are no published guidelines that explain how the Government assesses the validity of data requests – but most of the officials

24 Interviews. Luke Bawo, Thomas Davis, Dr. Ling Kituyi, and Augustine Kornyon. September 2015.

25 Interview. Augustine Kornyon, Data Coordinator for the International Rescue Committee. 24 September 2015.

26 During the epidemic, the Liberian MoH's Internal Review Board (IRB), the body charged with reviewing the ethics of research methodologies and information use according to domestic standards, shut down. According to researchers at Johns Hopkins, affiliated with Health Communication Capacity Collaborative (HC3), academic researchers used their home institutions' IRB. Interview. Anna Helland, Country Director, HC3 Project. 21 September 2015.

interviewed suggested that requests were granted based on the perception of the requester's intention and affiliation.[27]

International responder organizations, such as UNICEF, USAID, and MSF, also made requests to more sensitive data sources.[28] These requests were often for direct access to back-end databases, real-time information from mobile network operators, or personally identifiable health record information gathered from facilities. For more sensitive requests, the Government typically requires formal data sharing agreements. The data sharing agreement requirement has been controversial with responder organizations and politically complex to implement – meaning that very few have been operationalized:

> If it's with the WHO, it's a given based on their technical assistance role – it was more or less a mandate that the information management system shared information with them… Outside of them, it gets foggy. Can you routinely share raw data with MSF or CDC? So we grappled with those. We got repeated requests, but we stood firm and required a data sharing agreement – the question was who should sign it and I was a bit reluctant. Let it be a political decision.[29]

Political relationships are one of – if not the – most determinative factor in access to both information and funding support. One of the most illustrative, albeit anecdotal, examples of this dynamic comes from the recent USAID-sponsored conference on the interoperability of health information systems in Monrovia. The event was focused on building interoperable digital infrastructure for Liberia's MoH during an open solicitation for proposals aimed at exactly that issue, and was only open by invitation. This example isn't meant to criticize USAID's approach, but rather to demonstrate the natural tension between open technology systems and locally relevant operational coordination. The point at which information decisions reflect or affect authority and operations is also the point at which they become political.

The MoH is still building a structure to formalize and systematically share health information with third-party service providers.

Humanitarian Technology and the Disaster Market

During the peak of the epidemic, the volume of media coverage and its focus on the informational chaos attracted the attention and efforts of a wide range of conventional and unconventional groups. By the time the international community mobilized its resources – which happened after the peak of the outbreak – the active responders had already built a largely ad hoc information infrastructure. Those ad hoc systems served basic needs, but also created a significant amount of space for criticism - data commonly moved through advertising supported and unsecured

27 Interview. Joe Kerkula, Head of Social Mobilization for the Ministry of Health. 25 September 2015.
28 Interview. The Honorable Angelique Weeks, Chairwoman of the Liberian Telecommunications Authority. 24 September 2015.
29 Interview, Luke Bawo, Head of Information Management Systems, Ministry of Health. 26 September 2015

platforms, like e-mail and Google Fusion tables. Those criticisms fueled a wave of technocentric approaches, all of which needed on-the-ground partners and access to data from already overwhelmed infrastructure.

For all of the coordination flaws in the information systems implemented by the Government of Liberia and the international community, there was an even larger push from aspiring humanitarian technologists. A group of researchers found more than 300 separate initiatives to use messaging to engage communities in the affected countries – most of which were blasting messages out without even enabling two-way communication.[30] Two-way communication is fundamental to building trust and local impact – without the capacity for response, messages exacerbate the strain placed on infrastructure, attention, and legitimate sources of information. Not only were these information systems unresponsive, they were disconnected from the responders, meaning they didn't have any ability to answer questions, provide treatment, or even refer people to facilities that could provide treatment.[31] The majority of the coverage of both the issues and initiatives, even in reputable outlets, was remarkably uncritical.

Still, the coverage had the desired effect – it catalyzed an outpouring of funding from foundations, governments, militaries, scientific research organizations, and even mobile network operators.[32] For charitable organizations, the combination of money and popular media attention creates peak market conditions, which has the potential to distort programmatic focus and priorities. Dr. Ling Kituyi, who was the Foreign Medical Team Coordinator for the WHO, said:

> It was a whole cottage industry of people, even within WHO, who were trying to sell their apps. The most irritating part was one app that was designed to follow-up with people every day and get their data. Every day the person had to fill in their information… Why were we asking all these questions – it wasn't because we needed it, it was because all these people wanted their data.[33]

Luke Bawo was less diplomatic:

> I refer to it as a shark smelling blood in the water – if someone's wounded in the water, sharks smell it and start to circle… The international response to the emergency was to

30 Desiderio, Brandon "Fighting Fear and Stigma with Accurate Ebola Information." Ebola Communication Network (online) 19 August 2015: http://ebolacommunicationnetwork.org/fighting-fear-and-stigma-with-accurate-ebola-information/.

31 Although there were exceptions, even mobile projects that built partnerships in effected countries usually did so with content providers as opposed to healthcare providers. The differences were embedded enough that even GSM Association's Blueprint for Mobile Response to Ebola provides a broadcast, as opposed to service delivery model. "Blueprint: Ebola Mobile Response" GSMA Mobile for Development mHealth and Disaster Response (online) October 2014 http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/10/gsma-Ebola-Mobile-Response-Blueprint.pdf.

32 Sometimes, even on the same project. There was an unprecedented amount of funding from varyingly involved organizations to prove a justification for applying emergency exemptions to the legal and privacy protections that typically prevent the release of call detail records. One example: Bengtssson, Linus; Buckee, Caroline O.; Lu, Xin; Tatem, Andrew J.; Wetter, Erik; and Wesolowski, Amy. "Commentary: Containing the Ebola Outbreak – the Potential and Challenge of Mobile Network Data." PLOS (online) 29 September 2014: http://currents.plos.org/outbreaks/article/containing-the-ebola-outbreak-the-potential-and-challenge-of-mobile-network-data/.

33 Interview, Dr. Ling Kituyi, Foreign Medical Team Coordinator, World Health Organization. 18 September 2015.

> mobilize resources, so clearly it was a business opportunity for a lot of people.[34]

The most finite commodity in a disaster is the time and attention of the organizations that have an operational role in the response, especially after they've implemented "good enough" solutions. Despite the funder interest, the influx of app developers and big data analysts struggled to get the traction necessary to build an integrated or longer-term initiative with operational organizations. Notably, there was a small group of international organizations with the independent funding and political capital that enabled them to build medium-term technological projects – several of which gained significant traction as standalone information systems.[35] Outside of a few exceptions, however, technology-focused initiatives struggled to get legitimizing interest from operational organizations.

The Ebola response was neither fully analogue, nor fully digital – nor is it complete. The prominence of information technologies as components of the operational response, however, raises a host of new and traditional humanitarian response problems. The standardization of indicators, coordination of operations, and regularization of reporting – between and within response organizations – were significant problems before digitization. Each of these challenges is amplified by the complexity of new technologies, as are the incentives that compel humanitarian organizations to build market advantages over would-be collaborators.

One of the least-discussed elements of humanitarian information technology implementations is the significant legal risks posed by the collection, use, and international transfer of personally identifiable data. By virtue of their context, humanitarian interventions often occur in extra-legal gray areas, with varying degrees of propriety forgiven under the assumption of public benefit. These calculations often don't consider the necessity, proportionality, and efficacy of the tradeoffs made during times of emergency – each of which could play a role in a legal challenge. Without any check on the tendency to make short-term concessions that have long-term effects, international health and humanitarian organizations can over-reach and subject themselves to legal challenges from the very people they intend to help.

During the Ebola epidemic, the most prominent example of this kind of overreach was the call for mobile network operator records – usually called call detail records or call data records (CDRs) – in order to perform migration analysis and contact tracing.

34 Interview, Luke Bawo, Head of Information Management Systems, Ministry of Health. 26 September 2015.

35 One example is the "Dey Say" project implemented by UNICEF and Internews, in partnership with local media and the Liberian Red Cross Society to combat rumors. Although measuring impact is difficult with information systems, their engagement volume and process are being used to build disaster preparedness. Iacucci, Anahi Ayala "Combatting Rumors About Ebola: SMS Done Right." Medium (online) 26 March 2015: https://medium.com/local-voices-global-change/combatting-rumors-about-ebola-sms-done-right-da1da1b222e8.

Chapter 3: CDRs and Contact Tracing Ebola

CDRs include some of the most sensitive data that people generate, including location history, substantive communication history, and personal billing data. Despite that, there is very little evidence to suggest that CDRs, especially those that have been anonymized, are useful to track the spread of the Ebola virus. Nevertheless, the farthest-reaching, most common, and least interrogated requests for data during the epidemic were the international community's push for the release of CDRs to aid response efforts. This case study performs an in-depth investigation of the way that CDRs could be used to track Ebola, revealing that they're only useful when re-identified, invalidating anonymization as a balancing approach to privacy, and thus legal, protection. Not only are CDRs an ineffective way to track the Ebola virus, sharing CDR data likely violates data protection law.

In August of 2014, the MIT Technology Review published an article suggesting that mobile network data could be used to predict the spread of the Ebola virus.[36] The article drew on the work of Flowminder, a Swedish data science non-profit, and Caroline Buckee, a Harvard epidemiologist.[37] The idea and concept grew substantially from there – both in media coverage, complementary academic studies, and among development donors – leading to numerous requests for mobile networks and the Liberian Telecommunications Authority (LTA) to release CDRs. The most typical version of the request was that CDRs could be anonymized to reflect aggregated population movement, which could also be used to build predictive models about the spread of Ebola. More aggressive versions of those requests suggested that CDRs could be used to perform contact tracing to track the infected – and so mobile networks should open access to their core user databases to donor organizations. Over the course of September and October, coverage and pressure grew, and ultimately networks in Sierra Leone and Guinea did share CDRs.

In Liberia, the Liberian Telecommunications Authority (LTA) did not grant any requests to share CDRs with international and responder organizations.[38] According to the Honorable Angelique Weeks, Chairwoman of the LTA, concerns about the Ministry's capacity to manage and enforce data licensing environment were cause for caution. Despite requests from actors like USAID, NetHope, and UNDP, the LTA were closest to reaching an agreement with UNICEF – where, in exchange for the necessary hardware and training, they would create a real-time pipeline into the mobile networks' databases.[39] The contract included non-disclosure terms, data use limitations, and oversight by the

36 Talbot, David "Cell-Phone Data Might Help Predict Ebola's Spread." MIT Technology Review (online) 22 August 2014: http://www.technologyreview.com/news/530296/cell-phone-data-might-help-predict-ebolas-spread/.

37 Ibid.

38 Interview. Angelique Weeks, Chairwoman of the Liberian Telecommunications Authority. 25 September 2015.

39 Interestingly, UNICEF's mission focuses on the rights and protection of children – a group that has special privacy protections in both international and Liberian law. Interview. Angelique Weeks, Chairwoman of the Liberian Telecommunications Authority. 25 September 2015.

LTA – although it was apparently never executed.[40]

Unfortunately, very few of the articles or requests interrogated the need for migration data in depth – or whether any of the uses or justifying examples, bore comparison to the Ebola epidemic. Similarly, many of the calls for CDRs acknowledge that there are privacy implications – and policies that prevented their release – but largely presented them as afterthoughts, trivialities, or problems to be overcome in order to realize an obvious benefit. Understandably, in the face of an emergency, health and humanitarian responders will do nearly anything that seems as though it will help stem the growth of a disaster. That said, CDRs – especially when linked to health information – are some of the world's most sensitive data sources. Without a deeper investigation, it's extremely difficult to perform any kind of cost-benefit analysis – let alone evaluate the proportionality of the data release, explore what a data license to that information should look like, or consider the implications of international sharing and diffusion of provided CDRs. Even those analyses neglect the two, far more important considerations – namely, what are the laws that govern the sharing of CDRs, and is there any way to enforce them?

This chapter broadly analyzes the value of CDRs to contact trace Ebola – to be followed by an in-depth analysis of the applicable international, domestic, regulatory, and contractual frameworks that apply in the Liberian context.

Contact Tracing Ebola

Contact tracing is one of the most aggressive and manual ways that health systems track a disease. In its most basic form, it identifies an infected person and interviews them to track every person that they've been in contact with during the period they were contagious. Historically, it's an analogue process involving significant time from dedicated teams who interview the infected, visit the locations, interview and test others who have been exposed, and then repeat the process, to interview everyone the second person has been in touch with (provided they're positive for the virus).

Contact tracing is particularly effective for diseases that require direct contact with a contagious source in order to spread. Ebola is a hemorrhagic fever that's manually transmitted through bodily fluids, meaning that it is not as contagious as many other diseases. However, the virus causes victims to expel a wide range of fluids, meaning that contact in later stages of infection is extremely contagious, even after death. Ebola requires direct contact with the fluids of an infected person after they've begun exhibiting symptoms. Despite having a high mortality rate, Ebola is relatively difficult to transmit. For context, the R0 scale – the definitive system used to rate how quickly a disease spreads – gave the Ebola epidemic in West Africa a 1.51-2.53 rating, varying by country.[41]

40 Interview. Angelique Weeks, Chairwoman of the Liberian Telecommunications Authority. 25 September 2015.

41 Althaus, Christian L.; "Estimating the Reproduction Number of Ebola Virus (EBOV) During the 2014 Outbreak in West Africa," PLOS (online) 2 September 2014: http://currents.plos.org/outbreaks/article/estimating-the-reproduction-number-of-zaire-ebolavirus-ebov-during-the-2014-outbreak-in-west-africa/.

That means that each person infected was likely to infect an average of 2 additional people. For comparison, Measles has a R0 score of 18.[42] The rate at which Ebola spreads is important, but less important for this analysis than how it spreads. The way Ebola spreads determines what data points are useful predictors of additional infections.

During the Ebola epidemic, the international response put a significant focus on contact tracing. Like nearly every other aspect of the epidemic, the teams initially used paper-based records, realized the challenges involved, and transitioned to digital processes. Centrally, the WHO and the MoH brought in Dr. Hans Rosling, an international expert on data science and processes. Dr. Rosling built a small team to manually digitize the paper records that were collected from the Ebola Treatment Units (ETU), catalogue and then held daily briefings on the state of the epidemic.[43] Eventually, the county and district levels developed their own Data Officers, who ensured reporting and digitization into decentralized databases and then aggregated them into the national system.[44]

The digitization effort was not technologically sophisticated – it was manual data entry into a straightforward database system. The goal of the contact tracing effort was to build the database to the point where every newly identified case of infection came from someone whose name they had. Essentially, every victim that wasn't connected to a known source of infection meant that they didn't have a complete handle on sources of infection. Gradually, over the course of the response, the contact tracing database became more and more thorough – and it was only when all known cases came from known sources, all known cases were isolated and treated in ETUs, and there were no new cases for 21 days that the epidemic was called over. Even that process, though, is flawed, because it failed to account for factors for longer-term gestation. After Liberia was declared Ebola-free on May 9, 2015, 6 confirmed cases emerged after a man who had recovered from the virus transmitted it through sexual intercourse after a 7 week lull in new cases.[45] Liberia was declared Ebola free again on September 3, 2015.[46]

The other major digitization effort in the contact tracing practice focused on contact tracers – namely, giving contact tracers digital data entry tools so that the information collected was digital and portable from the outset. Given the large number of mobile and digital data collection tools, this particular opportunity was more sought-after and contested. According to Bawo, there were at least 9 separate contact tracing applications pitched to him – and he wasn't primarily responsible for that vertical of work.[47] The Liberian and international response community mostly responded to these pitches the same way they reacted to others – namely that they had "good enough" systems

42 Britton, Tom; Diekmann, Odo; Heesterbeek, Hans; "Mathematical Tools for Understanding Infectious Disease Dynamics," Princeton University Press, 2013 Chapter 7, pg. 161

43 Interview, Dr. Ling Kituyi, Foreign Medical Team Coordinator, World Health Organization. 18 September 2015.

44 Interview. Augustine Kornyon, Data Coordinator for the International Rescue Committee. 24 September 2015.

45 Farge, Emma; Toweh, Alphonso. "Liberia confirms new Ebola case as outbreak spreads" Reuters (online) 14 July 2015: http://www.reuters.com/article/2015/07/14/us-health-ebola-idUSKCN0PO1EN20150714.

46 "Epidemiological situation," European Center for Disease Prevention and Control (online) 13 September 2015: http://ecdc.europa.eu/en/healthtopics/ebola_marburg_fevers/Pages/epidemiological-situation.aspx.

47 Interview, Luke Bawo, Head of Information Management Systems, Ministry of Health. 26 September 2015

in place, and with few examples didn't adopt new tools after the peak of the epidemic. In November of 2014, Paul Allen organized the donation of 10,000 mobile phones, which were distributed to contact tracing teams, and added value – though providing scratch cards (the vehicle for delivering air time and messaging credit) was an ongoing challenge throughout the response.[48] That said, digitizing the existing work of the contact tracers, once implemented, made a sizable difference to the speed and efficiency of digitization.

This was the context for the call for CDR data.

CDRs

CDRs are a blanket term that refers to the data that mobile network operators collect in the course of providing telecommunications services.[49] Although practice varies between operators, in order to both provide services and present billing statements, network operators store a customer's name, address, billing status, account identifiers, payment information, log of incoming and outgoing phone calls, phone numbers attached to each call, length of each call, number of text messages sent and received, log of data use (including web sites visited, information transferred, apps used), and, where applicable, mobile money transactions history. Many mobile network operators record and store more information, but the above is typical.

One other piece of information that mobile network operators require is location data. Mobile network operators track location in two primary ways, depending on the type of phone and the user's privacy settings. The most common way is through towers – essentially, whenever a person uses a phone to communicate, it sends a signal to the closest tower or towers. The mobile network operator then triangulates location based on the speed at which that signal hits each tower. The accuracy of this method of location data is tied very closely to the density of the carrier's tower infrastructure – in places where there are lots of towers, there are lots of data points and location data is accordingly more reliable. In places where there aren't very many towers, for example, in rural West Africa, location is harder to triangulate.

48 "Paul G. Allen Commits to Enhancing Communication Capabilities in West Africa to Help Fight Ebola." Paul G. Allen Foundation, News (online) 17 November 2014: http://www.pgafamilyfoundation.org/news/news-articles/press-releases/enhancing-communication-to-fight-ebola. Even the Emergency Dispatch Unit (EDU), which manages the national emergency help line and routes ambulances and investigation teams, faces an ongoing shortage of scratch cards – they are temporarily provided by the International Committee of the Red Cross (ICRC), but that program is scheduled to stop operations in November of 2015. Interview, Dr. Ling Kituyi, Foreign Medical Team Coordinator, World Health Organization. 18 September 2015. Interview, Arthur Vaye, Head of the Emergency Dispatch Unit, 23 September 2015.

49 In some cases, the term CDR refers to the data set that is required to provide billing statements to customers. These definitions can vary between national jurisdictions, regulatory frameworks, and company standards.

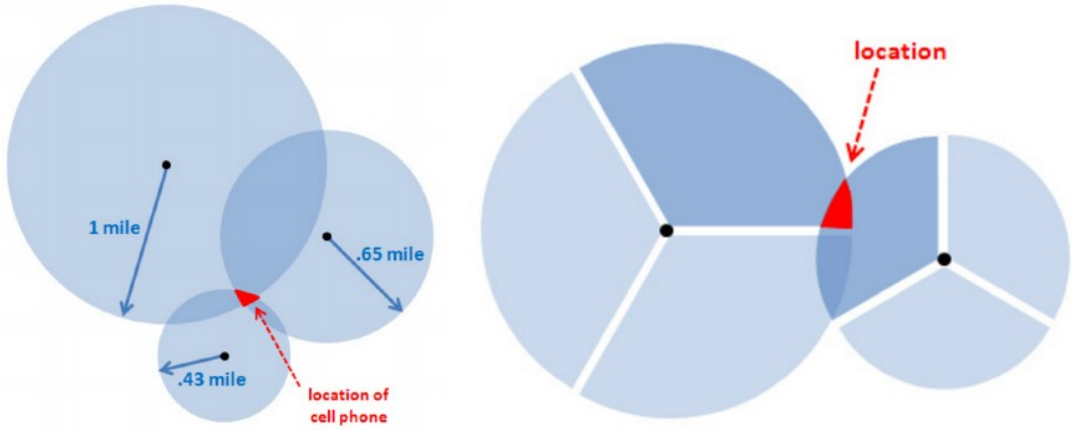

Diagram Credit: Chris Silver Smith, originally appearing in Search Engine Land, September 2008.

The second way that mobile operators track location data is through the Global Positioning System (GPS) which uses deviations from true time, measured through a series of satellites, to measure and track location. This method of tracking, while more accurate, depends on the user enabling location tracking through the phone or an application on the phone (common examples are Google Maps, Find My iPhone, and Uber). Each of these applications uses data signal to track user movement, sending data points to the infrastructure at rapid intervals and using the more continuous flow of data to refine location information.

When it comes to real-time location tracking of a large population, CDRs are undeniably the most effective, practical data source in the world. They are the most accurate and the most identifying of any data set that humans generate with any regularity. That is also why they are the most sensitive and have such a high potential for abuse. While this risk is noted in nearly all of the articles calling for the use of CDRs to augment contact tracing, none review whether they constitute a necessary data source to track Ebola.

Tracing Ebola with CDRs

Every virus is a little bit different, so every data model that built for tracking or predicting the spread of a disease needs to tailor to its unique characteristics. Ebola is a contact-based hemorrhagic fever, meaning that a person needs to have direct physical contact with the fluids of an infected person after they've become contagious – including after death.[50] Unlike many other diseases, particularly those that have airborne or non-human carriers (like Malaria, which travels largely through mosquitos), there are no ambient or environmental factors that predict the spread of Ebola. In addition, while the presence of people is a necessary precondition for the spread of the disease that concerns the epidemic response, the mobility and migration implications of the Ebola

50 "Implementation and management of contact tracing for Ebola virus," World Health Organization (online) September 2015 http://apps.who.int/iris/bitstream/10665/185258/1/WHO_EVD_Guidance_Contact_15.1_eng.pdf.

outbreak were largely overestimated.[51]

Flowminder's migration analysis using CDRs is the most broadly referenced justification for releasing CDRs to trace and predict the spread of Ebola, though the organization's primary assertion is that real-time mobility data would have been valuable as a means of building targeted and adaptable containment strategies.[52] While it's possible – and certainly applicable in emergencies with significant variations in movement patterns – there's a significant risk of overestimating the potential benefits of dynamic migration analysis of the transmission of this virus, held against the very real privacy costs of compelled CDR release. Even Dr. Linus Bengtsson, the Executive Director of Flowminder, is careful to nuance the significant way that virus transmission affects the importance of migration data to the data model:

> "If you're planning traffic, you need the whole picture to model the road. If you're trying to catch an individual traffic offender, the model of traffic can help – but it's really an entirely different ball game... With Ebola, you need to see the other person, which you don't see in the mobile data, so it's not as interesting [for Ebola] as for vector-born diseases... Just because you go to the same 100km/sq. area doesn't mean you met someone.[53]

There are personal identifiers and cultural behaviors that are more likely to correlate to the probability of the virus's spread, such as burial practices, which have a measurable impact on post-mortem transmission. Those datasets are often unavailable or highly dependent on correlation to other datasets in order to provide relevant insight (for example, maps of prevalence of cultural behaviors exist, but not in ways that directly document burial practices and the degree of direct physical contact involved in each). That use of burial practice information, however, clearly falls within the definitions of personally identifiable information – undermining assertions of the independent value of anonymized data in predicting the spread of Ebola. In other words, CDRs are only useful to Ebola contact tracing when they're re-identified or linked to personally identifiable information. As a question of data modeling, that increases the benefit of using a dataset like CDRs, as there aren't many other data sources that contain real-time relevant information for predictive modeling.

Ultimately, this simplifies the analysis of privacy, because it eliminates the presumption that anonymized data is useful to track or predict Ebola. There is no reason to believe that there are technological ways to ensure privacy in CDRs – both because of the necessary correlations and the

51 The early spread of Ebola from Guinea to Sierra Leone and Liberia is often cited as proof of the importance of "migration" patterns to the growth of the outbreak. Those examples, though, don't refer to group movements – they refer to individual movements. One could argue that group movements are a probabilistic model for individual movements, but that doesn't effect the need to use CDRs unless you also assume that the relevant authorities don't have knowledge of their highest traffic routes. In addition, simply knowing routes doesn't correlate to insight about specific epidemiological indicators without significant amounts of medically and personally identifiable information. Interview, Dr. Linus Bengtsson, Executive Director of Flowminder. 11 September 2015.

52 Bengtssson, Linus; Buckee, Caroline O.; Lu, Xin; Tatem, Andrew J.; Wetter, Erik; and Wesolowski, Amy. "Commentary: Containing the Ebola Outbreak – the Potential and Challenge of Mobile Network Data." PLOS (online) 29 September 2014: http://currents.plos.org/outbreaks/article/containing-the-ebola-outbreak-the-potential-and-challenge-of-mobile-network-data/.

53 Interview, Dr. Linus Bengtsson, Executive Director of Flowminder. 11 September 2015.

significant risks of re-identification. As a Brookings Institution white paper on mobile data collection in disease tracking said, “Best practices should accept that there are no perfect ways to de-identify data and there probably never will be.”[54] Recognizing that – whether by necessity or technological insecurity – CDRs are only useful to track Ebola as personally identifiable datasets. Dispensing with the fiction that anonymization is more than intermediary protection for data sharers, at least for the purpose of containing a contact-based virus, significantly simplifies the ethical and legal analysis.

The value of CDRs comes from correlation to personally identifying information, meaning that mathematical approaches to privacy risk mitigation that subsequently require re-identification are vehicles for managing liability. While that may be valuable for intermediaries as plausible deniability, it is, at best, a misleading statement about the intention and practice of digitally facilitated contact tracing and points to organizational and legal structures as the most realistic methods of managing data use, processing, and risks.

54 Kendall, Jake; Kerry, Cameron F.; and Montjoye, Alexandre de. “Enabling Humanitarian use of Mobile Phone Data,” Issues in Technology Innovation (online) November 2014: http://www.brookings.edu/~/media/research/files/papers/2014/11/12-enabling-humanitarian-mobile-phone-data/brookingstechmobilephonedataweb.pdf.

Chapter 4: Debatable Experimentation

The chaos of humanitarian disaster often creates an implied social license for experimentation with new approaches, under the assumption of better outcomes. Vested interests dominate the public discussion of humanitarian data modeling, downplaying the dangers of what is essentially a public experiment to combine mobile network data and social engineering algorithms. In the case of using mobile network data to track or respond to Ebola, the approaches are so new–and generally so illegal– that most advocacy focuses on securing basic access to data. Advocates for the release of CDRs often paint an optimistic picture of its potential benefits, without applying the same rigor to the risks or likelihood of harm. This trades on the social license created by disaster to experiment with the lives of those affected, under the implicit assumption that it can't make the situation worse.

The problem is that personally identifiable data in the wrong hands can make many situations worse. Once released, data is nearly impossible to control or "take back", meaning that once released CDRs create risks immediately that last indefinitely. During and after a disaster, there are substantial benefits to having access to CDRs in humanitarian and commercial contexts. The value of these data sets, and the rights of the people they represent, should increase the ethical concerns and scrutiny of access negotiated under the auspices of humanitarian and development contexts. In the Ebola response, it did just the opposite.

Data modeling may have significant benefits, but most publicly funded social interventions bear the burden of proving those benefits before compromising the human rights of millions of people. To date, there simply hasn't been nuanced enough experimentation, analysis, or debate about what factors lead to data modeling having a positive social impact that addresses specific threats or issues. The debate about the humanitarian use of data models not only has that burden not been met, there aren't even the appropriate research, licensing, and oversight mechanisms to evaluate and protect against potential harms. Without more research, the forced release of mobile network data may not only endanger the lives of the people humanitarians seek to serve – they may expose humanitarian organizations to a new kind of legal risk.

Calls for CDRs seems to gain the most traction during times of emergency, which also has the potential to set norms in circumstances that distort the cost-benefit analysis away from individual rights and agency. This chapter will explore the state of the institutional debate, in order to understand the incentives and actors involved in defining the legal and practical exercise of digital emergency powers.

The Endlessly One-Sided Debate

The debate over the best-fit way to collect, share, and use CDRs is still in its very early stages. The conversation about appropriate use of mobile network data, as of now, is largely comprised of single perspective advocacy pieces, each of which advance an organizational or commercial interest. The institutional debate focuses on advancing the interests of that group's primary constituency, but fails to prove where CDR-based data modeling creates uniquely actionable enough insights to justify their release.[55] Most recommendations on policy, institutional frameworks, and technological innovation focus on limiting the risk inherent in sharing of CDRs. Conspicuously absent is a critical discussion that acknowledges the experimental nature of data modeling in emergency response and social engineering, with a primary emphasis on quality control, public understanding, and human rights.

Although there have been several high profile discussions at large events, the conversations that matter – the private negotiations that underpin the contracting, sharing, and use of mobile network data – tend to happen behind closed doors. That's not uncommon for emerging areas of practice – but in the case of the compelled release of CDRs, the costs and benefits have broader public implications than typical public-private partnerships. Once given, a grant of access to data is nearly impossible to limit – data can be copied and shared in ways that no technical or legal infrastructure is able to effectively regulate.

The World Economic Forum (WEF), the GSM Association, MIT, and UN Global Pulse have advanced the institutional discussion of emergency mobile network data management. Each organization has contributed instructive analyses of the operative elements of and barriers to using CDRs, with recommendations aimed at their constituent audiences. The WEF convened a group of industry experts to discuss the subject of data privacy in emergency response in November of 2014, resulting in a series of broad suggestions toward developing harmonized legal, operational, and policy frameworks to facilitate the "controlled" use of phone data by "trusted third parties."[56] The GSMA's recommendations advocate limiting access to both information and the database itself – promoting the mobile network operator as a supervisor or privacy practices or the data processor, which shares limited data based on specific queries.[57] UN Global Pulse's publications provide a high

55 A significant number of the explanations of CDR value focus on their comparative timeliness to census data – especially in places where census data is difficult to access. While that's undoubtedly true, national censuses come with a significantly more explicit and robust consent and licensing infrastructure – as well as a publicly accountable institution in the event of abuse. While there are variations on implementation in practice, the comparative value doesn't inherently justify the abrogation of the underlying consent requirements, licensing infrastructure, or publicly accountable management institutions. Hern, Alex, "Mobile phone records could help the fight against Ebola, study finds," The Guardian, Technology (online) 29 October 2015: http://www.theguardian.com/technology/2014/oct/29/mobile-phone-records-help-fight-against-ebola-study-finds.

56 The paper referenced was published by the Brookings Institute, but featured in the WEF's annual event. Although there was more discussion Kendall, Jake; Kerry, Cameron F.; and Montjoye, Alexandre de. "Enabling Humanitarian use of Mobile Phone Data," Issues in Technology Innovation (online) November 2014: http://www.brookings.edu/~/media/research/files/papers/2014/11/12-enabling-humanitarian-mobile-phone-data/brookingstechmobilephonedataweb.pdf.

57 "GSMA guidelines on the protection of privacy in the use of mobile phone data for responding to the Ebola outbreak," GSMA Mobile for Development (online) October 2014: http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/11/GSMA-Guidelines-on-protecting-privacy-in-the-use-of-mobile-phone-data-for-responding-to-the-Ebola-outbreak-October-2014.pdf.

level review of approaches that may be useful – including mathematical anonymization, privacy frameworks, and data minimization – but conclude that the value of the insights gained exceeds the risks or threats of prioritizing privacy over use.[58] Each report is a proactive institutional acknowledgment of the potential value of network data and the countervailing concerns about privacy.

Variable Public Good

The tension between the rights of the individual and the public good in times of emergency understandably skews toward the collective interest, but the institutional debate includes assumptions that are worth interrogating in greater depth. The core value proposition is that publicly accessible CDRs – or at least the distribution of CDRs to "trusted" organizations – will return efficiency gains in emergency response and public services that serve the public good. The institutional debate uses a small number of case studies that demonstrate the value of real-time mobility data to public service initiatives, but there's no analysis of the underlying factors that create that value. In addition, mobile network data isn't necessarily consistent – it can vary by continuity of SIM ownership, tower location logging (which can vary based on the availability of electricity), and consent.[59] Even ignoring data quality and modeling issues, there are an enormous number of extant variables - such as responder adoption, type of humanitarian response (i.e. – civilian vs. military), and biases inherent in any statistical construction, among many others – that effect how we define or achieve public good using CDRs and data models.[60]

The question of whether an intervention serves the public good isn't binary, it also raises practical ethical questions about what bias or population it favors. Focusing on digital data sources could skew the representative quality of the data and target disaster assistance resources toward communities that are capable of producing data. These concerns get more complicated in regions like West Africa, which has significant digital and data divides between urban and rural areas. These divides not only have social policy and privacy implications – they also underline how many variables there are when experimenting with data modeling in emergency and social service engineering.[61]

58 "Mobile Phone Network Data for Development," UN Global Pulse (online) October 2013: http://www.unglobalpulse.org/sites/default/files/Mobile%20Data%20for%20Development%20Primer_Oct2013.pdf.

59 A number of customers, for example, are able to opt-out of third-party and promotional messaging, including participation soliciting messages from international organizations. According to CellCom executive, the opt-out list is dominated by the "top of the pyramid," automatically skewing results. Interview. Fabian Ochanda, Sales Director for CellCom. 21 September 2015.

60 According to the GSMA's Pat Walshe, director of data privacy, operators were flooded with requests that didn't have attached information about use case, whether data would inform or integrate with response efforts, or limitations on data use that could form the foundations of a license. Schenker, Jennifer L. "Ebola: How Big Data Failed to Help Curb its Spread," Informilo (online) 2 March 2015: http://www.informilo.com/2015/03/ebola-how-big-data-failed-to-help-curb-its-spread/.

61 For a considerably deeper exploration of the benefits and costs of adopting algorithmic data modeling for social systems, particularly around decision-making support, consider: Colin, Jean-Noël and Rouvroy, Antoinette "Of Data and Men: Fundamental Rights and Freedoms in a World of Big Data." Council of Europe (online) 17 September 2015 available online: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR(2015)09_Big%20data%20draft%20report%20170915_A.%20Rouvroy%20et%20J-N%20Colin_DRAFT_En.pdf.

Even Flowminder's Dr. Bengtsson is a vocal advocate for a more nuanced and experimental approach to data modeling for social and disaster response engineering:

> "There's a lot of potential, but any kind of application in public health or social engineering should be based on thousands of academic papers and decades of professional experience. In disaster response, you can maybe do a lot of quite good things early on, but then it's a process of research and modeling and improvement... People think that you have the data and then it tells you everything, but that's just not the case. In Nepal, we've had 7 PhDs working around the clock since April and everyone is still frustrated because there's a lot of work to do and we want to improve the analysis further.[62]

The variations in data model design and effectiveness may justify the call for more experimentation – but they don't necessarily justify the application of untested or insecure approaches in fragile and vulnerable contexts.[63] Not only do we not have good justifications for the application of experimental practices, we don't have the institutional infrastructure for public evaluation and oversight of the use of CDRs. There are no publicly appointed bodies or auditing processes to assess the contextual value of a particular data model. Without transparent mechanisms, we aren't able to measure or review whether any of the predictive models actually deliver improved outcomes. Building mechanisms that create broader understanding, trust, and critical analysis of data models, especially through the lens of public policy and human rights, will be an important part of justifying the release of CDRs for public benefit.

Digital Emergency Power

Although there are a significant number of ways to structure the release of CDRs, most of the public calls for openness have been direct appeals to mobile network operators and governments. In both cases, releasing personally identifiable information absent customer consent is an extra-legal action, requiring governmental sanction. During times of emergency, the government is typically the authority compelling the release or receiving CDR data. Governments can share or delegate information and assets to third parties, but usually only within limitations that attach public accountability to that delegation. Compelling the release of CDRs, no matter the purpose or use, is an exercise of emergency power – which invokes a wide range of legal issues, especially for third parties that act as quasi-governmental bodies.

Calls for CDRs, even when they recognize the experimental nature of mobile data in social and

62 Flowminder's Nepal work is not related to Ebola - it's related to a disaster which has more migration-based implications. The quote is offered for reference on the difficulty of building useful and accurate statistical models for disaster circumstances. Interview, Dr. Linus Bengtsson, Executive Director of Flowminder. 11 September 2015.

63 The two most-cited case studies from Flowminder's work are disaster response in the Haiti earthquake and the spread of Malaria in Kenya. Both of those examples had significant migration implications, based on population movements or vector-borne illness risk factors, respectively. In each of those cases, mobility plays a different role in designing an effective response – whereas in Ebola contact tracing, mobility data is only useful in concert with personally identifiable information. Talbot, David "Cell-Phone Data Might Help Predict Ebola's Spread." MIT Technology Review (online) 22 August 2014: http://www.technologyreview.com/news/530296/cell-phone-data-might-help-predict-ebolas-spread/.

public health systems, gloss over the significance of the inherent costs of facilitating that experimentation. Specifically, releasing CDRs infringes on the property and human rights of the people who generate, and therefore own, the underlying data. In addition to ownership and privacy rights, the release of personally identifiable data creates a significant and indefinite amount of risk to the individuals affected. At the moment, however, the only way to seek protection is through the legal system. The legal systems and regulatory authorities charged with monitoring and enforcing data protection laws– even when they have implementation frameworks– continue to struggle with the technological complexity and significant costs of enforcement of licensing personally identifiable information.

Chapter 5: The Law

For the most part, how the humanitarian community acquires, moves, uses, stores, shares, and publishes data is likely illegal. The non-governmental use of CDRs is so illegal that most writing advocating for their use cite the law as a major obstacle for continued experimentation. Awareness does not mitigate illegality, however. The most commonly discussed legal risks draw from telecommunications, privacy, and data protection laws, but current humanitarian practice could also implicate property, libel, and due process laws. The differences and conflicts between these laws run the risk of compounding, as opposed to mitigating, the liability faced by international humanitarian organizations. An international organization can be brought before courts, tribunals, and regulatory authorities anywhere they operate–and conviction in one jurisdiction doesn't protect that same organization from multiple suits for the same case or practice.

The most common defense humanitarian data advocates offer is that CDRs are anonymized prior to sharing, and therefore aren't subject to data protection laws. However, the impossibility of complete anonymization, particularly as more data is released, belies this argument. Commercial telecommunication regulations and data protection laws, prohibit the sharing or seizure of personally identifiable information with or by any party other than the government, especially absent licensing and enforcement mechanisms to protect those affected. While these legal protections are inconvenient for organizations seeking to experiment with emergency response contexts, they do play an important role in the protection of human and property rights.

This analysis identifies and explains the most prominent legal frameworks relevant to the Ebola response in Liberia, but it is not comprehensive. Humanitarian organizations are likely subject to an enormous range of laws, regulatory regimes, and digital authorities outside of Liberia and ECOWAS that create additional causes of action, depending on the circumstances and affected parties. For example, children have heightened privacy protections in international law – meaning that any organization focusing on children may be subject to heightened scrutiny or consequence.[64] Similarly, a number of legal entities – including the United States and European Union – have laws that govern the way that organizations registered within their jurisdictions treat civil tort liability, data privacy, and human rights wherever they operate. As a result international organizations and officers that receive or user of data illegally may be subject to litigation in their country of origin, as well as the country where the data was acquired. Some of those entities also have long-arm jurisdictional laws, such as the Alien Tort Claims Act, which could be applied to bring suit against mobile network operators that violate the human rights of their citizens, as enunciated in international law.

64 These rights broadly emanate from the Universal Declaration of Human Rights, and its subsequent amendments and interpretations, including the UN Convention on the rights of the child.

These long-arm lawsuits are most likely in cases where the release, processing, or use of CDRs is alleged as a potential or partial cause of damages to a person's health, freedoms, or identity.

There is also a rapidly evolving body of law that regulates the transfer of data across national or regional boundaries, which may form the foundation of civil causes of action in a wide range of sovereign jurisdictions and non-governmental fora. Similarly, academic institutions have their own standards for treatment of personally identifying information inline with their own ethical and Internal Review Boards, which operate independently – and create separate causes of action within their designated adjudication systems.

This chapter highlights some of the international treaties, domestic laws, and regulations that apply to the governmentally compelled release of CDRs in Liberia in the context of the Ebola response. It's important to note that the identity of the parties in question determines the cause of action, applicable laws, and venue. This analysis will focus on the causes of action available to individuals or groups of users based on the release of CDRs.

This chapter will review causes of action against the mobile network operator and the Government of Liberia – the two most influential actors and likely defendants – though third party organizations could be included under domestic or international law, especially in the event. The two most likely causes of action are: (1) violation privacy and data protection; and (2) unjust deprivation of property rights.

While this is an analysis of law, neither its substance nor its conclusions are intended as legal advice and anyone considering or actively involved in legal action on this or other issues should seek counsel from an appropriately qualified attorney prior to taking action.

International Privacy Law

The right to privacy in international law emanates from Article 12 of the Universal Declaration of Human Rights, which grants people the ability to challenge "arbitrary interference with his privacy," a protection which is echoed in subsequent laws, like the International Convention on Civil and Political Rights (ICCPR).[65] These set the conceptual tone for privacy and the right to protection from its violation, though did very little to define the concept or implementation procedures. The Charter of Fundamental Rights of the European Union added data as a core component of modern privacy protection - including a duty to protect, the requirement of equanimity in use for a lawful purpose, a right of access to data about oneself, the right to correct, and, most importantly, the requirement of user consent.[66] All of this set up the most influential data protection law in the

65 Universal Declaration of Human Rights (1948), Article 12, available online: http://www.un.org/en/documents/udhr/ and The International Convention on Civil and Political Rights (1976), Article 17 (1-2) available online: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

66 The Charter of Fundamental Rights of the European Union (2000), Article 8 available online http://ec.europa.eu/justice_home/fsj/rights/charter/fsj_rights_charter_en.htm.

world, the Council of Europe's Data Protection Convention 108 and its Additional Protocol.[67]

ECOWAS' Supplementary Act

Convention 108 is the legal precedent and foundation for the Economic Community of West African States' (ECOWAS) Supplementary Act on Personal Data, the preeminent regional legislation that governs the collection, processing, and application of data.[68] The ECOWAS Supplementary Act is based in part on Convention 108 and partially based on the African Charter on Human and Peoples' Rights.[69] The most relevant portions of the Supplementary Act provide for (1) The Data Protection Authority; (2) Data Processing and Controller Limitations; and (3) Data Subject Rights.

The Data Protection Authority

The ECOWAS Supplementary Act is one of the most formidable data protection laws in the world, architecting a framework for data rights, enforcement, and adjudication. The Supplementary Act compels the creation of a national Data Protection Authority (DPA) within each ECOWAS state, an independent, legally immune body that cannot share members with the government.[70] The DPA has a broadly construed authority, including proactively informing digital service users of their rights; review emerging data collection, processing and use methods; and educate and consult stakeholders, including opinion seekers, each branch of government, and international regulators.[71] The Supplementary Act specifically grants the DPA the authority to monitor and enforce human rights data protections during an emergency.[72] The DPA is able to issue injunctive orders, sanctions, and fines in response to human rights violations – including the ability to prevent transfer and use of specific data processes or pieces of personally identifiable information.[73] In other words, a DPA is the explicit, dedicated organization to define and police the issues raised by data collection, processes, and use during emergencies.

Data Processing and Controller Limitations

The Supplementary Act outlines the rights framework for the use of data – including the obligations of data processors (parties that use data) and unacceptable types of use. The Supplementary Act creates a proactive consent requirement for personal data, though it also creates exceptions for the execution of a "public interest mission or relevant to the exercise of public authority that is

67 Greenleaf, Graham. The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108. International Dave Privacy Law, Volume 2, Issue 1 (2012) available at: http://idpl.oxfordjournals.org/.

68 Ibid.

69 Kuner, Christopher. "Extraterritoriality and the Fundamental Right to Data Protection," Blog of the European Journal of International Law (online) 16 December 2013: http://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/.

70 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Chapter IV. Abuja. 16 February 2010 (online) http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

71 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Chapter IV. Article 19. Abuja. 16 February 2010 (online) http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

72 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Chapter IV. Article 19 (3). Abuja. 16 February 2010 (online) http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

73 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Chapter IV. Article 19 (3) a-c and Article 20(1-3). Abuja. 16 February 2010 (online) http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

vested in the data controller or the third party to whom the data is disclosed," as well as for "safeguarding the fundamental interests... of the data subject."[74] The Supplementary Act also requires proportionality and limited use provisions, ensuring that the data is obtained for "specified, explicit, and lawful purposes and shall not be further processed," and "shall be kept for a period which shall not exceed the period required for the purposes for when they were obtained."[75] In addition to creating use limitations, the Supplementary Act prohibits receiving or processing personally identifiable data, though it creates exemptions for consent, public interest, and certain non-profit activities (although they require consent).[76] The Supplementary Act imposes additional prohibitions against transmitting personally identifiable information outside of ECOWAS countries, requiring that the receiving country have commensurate data rights protections and direct notice to the DPA.[77] There are also strong prohibitions against "direct prospecting, which is defined as,

> any message sent, on whatever medium and of whatever nature, in particular a commercial, political, or charitable message, aimed at promoting, directly or indirectly, goods, services or the image of a person selling goods or providing services.[78]

Lastly, and perhaps most determinatively, the Supplementary Act also states:

> No decision that has legal effect on an individual shall be based solely on processing by automatic means of personal data for the purposes of defining the profile of the subject.[79]

The Supplementary Act creates a strong domestic ownership and user consent framework, as well as the outlines of data licensing and public purpose exemptions. The broad constructions of public purpose convey significant interpretive latitude, but also include restrictions on the influence that can be attributed to data processes.

---

74 This language is probably broadly construed enough to waive both governmental and third-party requirements for consent, provided there was a sufficiently defined and bound relationship established by the data sharing agreement between the mobile network operator and the Government. Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Chapter V, Article 23(1) and (2)b and (2)d. Abuja. 16 February 2010 (online) http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

75 The act also creates a longer term exception for research – though it doesn't specify how consent or ongoing use limitations attach. Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Chapter V, Article 25(1) and (3). Abuja. 16 February 2010 (online) http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

76 The public purpose exemption is the most applicable here – as is its trickle down applicability to relevant third parties. There are also readings of the legal and regulatory compliance exemption that may apply. Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Chapter V, Article 30 and 31(3),(6), and (8). Abuja. 16 February 2010 (online) http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

77 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Chapter V, Article 36. Abuja. 16 February 2010 (online) http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

78 As a prohibition, this likely creates a cause of action against any humanitarian or health organization that uses data obtained during the emergency – including photographs – as a component of their marketing, both to Liberians and to international donor relationships. Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Chapter V, Article 36. Abuja. 16 February 2010 (online) http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

79 The applicability of this provision relies on an adjudicators' interpretation of the term "solely," which is problematic for a number of reasons. The suggestive power of algorithmically constructed analyses has been noted at length and, in this specific context, Colin, Jean-Noël and Rouvroy, Antoinette "Of Data and Men: Fundamental Rights and Freedoms in a World of Big Data." Council of Europe (online) 17 September 2015 available online: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR(2015)09_Big%20data%20draft%20report%20170915_A.%20Rouvroy%20et%20J-N%20Colin_DRAFT_En.pdf.

Data Subject Rights

The ECOWAS Supplementary Act also establishes rights for data subjects (the party who creates the data). Data subjects are entitled to being informed, no later than the time of collection, that their data is being used, as well as the characteristics of that use.[80] Subjects should be informed of the identity of the organization processing their data; the purpose of that processing; any third parties receiving personal data (or any derivative thereof); their rights to access, correct, or redact personal information; the amount of time the organization will preserve data; and the possibility of any transfer to another country.[81] In addition to notice requirements – which essentially include the terms of the license that data, even if not negotiated – data subjects have the right to access personal data, to object to its use by a processor, to rectify any flaws in personal data exchanged, and to request its destruction.[82]

The ECOWAS Supplementary Act is the guiding framework for domestic data and digital privacy frameworks in Liberia – and was signed into law by President Ellen Johnson Sirleaf in 2010. ECOWAS treaties, human rights laws, and any disputes that result from them, are adjudicated by the ECOWAS Community Court of Justice (CCJ).[83] The CCJ construes its jurisdiction broadly and will hear cases brought by individuals for violation of their human rights, as well as by national courts that refer domestic cases for appellate judgment based on the interpretation of ECOWAS agreements.[84] In other words, individuals wishing to challenge whether the Government of Liberia's use of data, or the third party use of data based on Government facilitation, violated their human rights could choose the CCJ as a venue.

Liberian Privacy Law

Liberia's domestic legal frameworks reference privacy, but apply protections within regulatory contexts, as opposed to establishing over-arching definitions or enforcement mechanisms. The Liberian Constitution establishes a right to privacy and requires a court order for any exemptions.[85] The Constitution also includes non-interference with telecommunications as a component of freedom of speech.[86] The other relevant provisions in the Constitution relate primarily to detention and expropriation, though they focus on ensuring due process of law, as opposed to evaluating the downstream effects of privacy violations.

80 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Chapter VI, Article 38. Abuja. 16 February 2010 (online) http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

81 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Chapter VI, Article 38(1-8). Abuja. 16 February 2010 (online) http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

82 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Chapter VI, Article 39-41. Abuja. 16 February 2010 (online) http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

83 "ECOWAS Community Court of Justice," Open Society Justice Initiative (online) June 2013: https://www.opensocietyfoundations.org/fact-sheets/ecowas-community-court-justice.

84 Ibid.

85 The Constitution of the Republic of Liberia (1986) Article 16 available online http://www.tlcafrica.com/constitution-1986.htm.

86 The Constitution of the Republic of Liberia (1986) Article 15(b) available online http://www.tlcafrica.com/constitution-1986.htm.

Liberia also protects the specific rights of particular groups, such as children, which are implicated by the use of CDRs. Here, a significant amount hinges on whether CDRs are considered 'personally identifiable information,' – though, as described above, anonymization in the context of Ebola tracking or prediction is, at best, an interim state toward creating personally identifiable datasets. CDRs, even if anonymized, inevitably include additionally protected information from minors. The law most relevant to the definition, protection, and enforcement of privacy as it manifested through CDRs is the Liberian Telecommunications Act of 2007 (LTA 2007).

Liberian Telecommunications Act of 2007

The LTA 2007 is the legislative foundation of Liberia's mobile telecommunications industry, which also establishes and defines the Liberian Telecommunications Authority.[87] Privacy and the protection of customer information are one of the defined Purposes of the LTA 2007, and it establishes steep punishment for the violation of privacy – such as removing the license of a mobile network operator.[88] In addition, the LTA 2007 specifically prohibits mobile network operators from collecting, using, maintaining, or disclosing customer data except as necessary to bill that customer – and even then, only for a period of 12 months.[89] The LTA 2007 also requires that a mobile network operator disclose any and all purposes for data collected to the user in advance and, unless otherwise provided for by law, get consent.[90] One reading of the LTA 2007 suggests that it is illegal to collect, use, or maintain tower-based location data as it correlates to individual accounts, regardless of whether it is ever shared with the Government or a third-party.

Assuming that it is legal for mobile network operators to collect, use, and maintain location records attached to specific user accounts, the operative questions of law relate to informed user consent prior to collection and the justification of sharing those records with the Government. Absent written consent, mobile network operators are explicitly prohibited from sharing identifying information with anyone other than the government – making all direct information sharing with third parties (like international organizations or NGOs) illegal.[91] This also means that absent government intervention, any customer that can prove that their data was shared with a third party

87 Liberian Telecommunications Act of 2007 available online: http://www.lta.gov.lr/doc/LiberiaTelecommunicationsAct.pdf.

88 Liberian Telecommunications Act of 2007, Section 3(g) and 20(1)(b-d) available online: http://www.lta.gov.lr/doc/LiberiaTelecommunicationsAct.pdf.

89 This raises separate legal questions about whether location data is necessary to provide accurate billing statements to customers – and whether there is a distinction between pre-paid and post-paid customer billing requirements. The significant majority of the Liberian mobile customer base operates on pre-paid accounts, meaning that there are no contracts and that billing is done through deduction against a standing balance. In these billing relationships, there is no line-item presentation of calls or communications, and therefore no obvious need to have location data. Tower records are, of course, necessary and valuable for the overall operation and maintenance of mobile services, but not as they attach to any form of single user or account. In order to understand user movement, however, location information would need to attach to a single account, which means that correlation identifies it as customer data, not network maintenance data. Liberian Telecommunications Act of 2007, Section 48(3) and 49(1-3) available online: http://www.lta.gov.lr/doc/LiberiaTelecommunicationsAct.pdf.

90 Liberian Telecommunications Act of 2007, Section 49(1-3) available online: http://www.lta.gov.lr/doc/LiberiaTelecommunicationsAct.pdf.

91 Liberian Telecommunications Act of 2007, Part X, Section 49(1) available online: http://www.lta.gov.lr/doc/LiberiaTelecommunicationsAct.pdf.

can bring suit against the responsible mobile network operator.[92] In addition to court-imposed sanctions, the Liberian Telecommunications Authority can levy punitive fines against any mobile network operator found to violate this law, independent of damages assessed to an individual plaintiff.

Consent Requirements

The LTA 2007 includes a number of informed consent requirements, including providing clear data collection and use purposes and limitations.[93] Contrary to the terms of the LTA 2007, neither of Liberia's major mobile network operators explicitly provide their mobile Terms of Service Agreements on their websites.[94] Further, pre-paid service customers, which make up the majority of the subscriber base, don't sign Terms of Service Agreements.[95] Even when customers do receive Terms of Service Agreements, they don't include any notifications or limitations on data use.[96] As a standalone practice, this is a violation of the LTA 2007, as well as nearly every subsequent piece of legislation that affords user rights, like the Consumer Bill of Rights and the New Consumer Guidelines.[97] The absence of Terms of Service Agreements, both in typical business practices, as well as on their websites, is an explicit violation of the LTA 2007.[98]

Further, failing to inform a customer about any purpose for data collection makes it illegal for a mobile network operator to collect maintain or share any information that is not otherwise required by law. Without even boilerplate legal language establishing "any legal purpose" use, it's not clear that mobile network operator data collection that falls outside of SIM card registration or billing requirements is legal. It's important to separate the legality of collection, use, and maintenance from the legality of sharing – both of which require consent. However, if a mobile network operator doesn't have consent for the former, questions of the legality or definition of sharing practices become moot, except as additional violations.

Government Intervention

The LTA 2007 creates broad rights for the Government of Liberia to access customer information,

92 In the event that customers are unable to resolve their dispute with the mobile network operator, they may refer the matter to the LTA for mediation prior to or in lieu of bringing a case before the court. Liberian Telecommunications Act of 2007, Part XV, Section 74(1) available online: http://www.lta.gov.lr/doc/LiberiaTelecommunicationsAct.pdf.

93 Liberian Telecommunications Act of 2007, Part X, Section 49(1) available online: http://www.lta.gov.lr/doc/LiberiaTelecommunicationsAct.pdf.

94 As reviewed 31 September 2015. Lonestar MTN available online: http://www.lonestarcell.com/ and CellCom available online: http://www.cellcomgsm.com/.

95 Interview. Fabian Ochanda, Sales Director for CellCom. 21 September 2015.

96 Based on Terms of Service Agreements received from Liberian operators, confirmed by the interview with Fabian Ochanda. Interview. Fabian Ochanda, Sales Director for CellCom. 21 September 2015.

97 The Consumer Bill of Rights includes the following language: "Consumers must be protected from improper use of information by service providers in the course of providing telecommunications service. It is required of service providers to protect the privacy of financial, personal, and other confidential information on consumers..." Liberian Telecommunications Act of 2007, Part X, Section 51 available online: http://www.lta.gov.lr/doc/LiberiaTelecommunicationsAct.pdf; New Consumer Guidelines (18 March 2013) available online: http://www.lta.gov.lr/doc/New%20Consumer%20Guidelines%20.pdf; and Consumer Bill of Rights (18 March 2013) available online: http://www.lta.gov.lr/doc/Consumer%20Bill%20of%20Rights%20.pdf.

98 Liberian Telecommunications Act of 2007, Part X, Section 55-56 available online: http://www.lta.gov.lr/doc/LiberiaTelecommunicationsAct.pdf.

although these rights are largely subject to emergency exemptions and criminal due process.[99] The Ebola epidemic is an exceptional circumstance in that it skirts the line between a national security priority and a declared public health emergency, which are the two included types of emergency powers. In the event of a national security threat, Government access to private information requires an order from the Attorney General – though once issued, it creates completely unfettered access to a mobile network operator's infrastructure with complete indemnification.[100] Powerfully, the Attorney General can grant real-time access to the mobile network operator's database, which is neither anonymized nor filtered to a specific type of data. This authority could also conceivably create the freedom to share information with third party service providers or responders, though there is no explicit language or precedent to inform the decision either way. Similarly, there is nothing to suggest that the Attorney General of Liberia issued an order during the Ebola epidemic to let this happen, although it was within his authority to do so.

In the event of an emergency, the LTA 2007 gives the Ministry coordinating the emergency response the authority to create rules for the provision of telecommunications services, but does not grant the same, direct access to mobile network operator infrastructure.[101] The invocation of public emergency powers also does not indemnify the mobile network operator or the Government from human rights abuses. Emergency power invocation also enables mobile network operators to submit an application for cost-recovery based on any expenses or operational costs incurred as a part of the response.[102] Interestingly, in the case of the Ebola response, the legal authority conferred to the Government is limited to the Ministry coordinating the response – namely the Ministry of Health, not the LTA. This is likely an insignificant distinction, but does raise the question of the intended legal role of the LTA as a component of the disaster response infrastructure. The use of emergency powers does not explicitly create the authority to share information with third party organizations, nor does it protect any organization involved from subsequent litigation.

The Data Protection Authority That Wasn't

By virtue of its participation in the ECOWAS Supplementary Act, the Government of Liberia is obligated to create a Data Protection Authority, with the full mandate, operational authority, and enforcement powers described above. The LTA has draft legislation that has gone through significant drafting and review, though it has never been implemented.[103] This Authority, as established, provides significant legal and operational clarity to data protection practices in

99 Liberian Telecommunications Act of 2007, Part X, Section 52 and Part XIV Sections 69-71 available online: http://www.lta.gov.lr/doc/LiberiaTelecommunicationsAct.pdf.

100 Liberian Telecommunications Act of 2007, Part X, Section 52 and Part XIV Sections 69-71 available online: http://www.lta.gov.lr/doc/LiberiaTelecommunicationsAct.pdf.

101 Liberian Telecommunications Act of 2007, Part XIV Sections 70 available online: http://www.lta.gov.lr/doc/LiberiaTelecommunicationsAct.pdf.

102 Liberian Telecommunications Act of 2007, Part XIV Sections 70(2) available online: http://www.lta.gov.lr/doc/LiberiaTelecommunicationsAct.pdf.

103 Interview. Angelique Weeks, Chairwoman of the Liberian Telecommunications Authority. 25 September 2015.

Liberia, especially during times of emergency. As it stands, according to the Honorable Angelique Weeks, Chairwoman of the LTA, "There are no [specific] regulations in place for data privacy."[104]

Liberian Property Rights

In addition to the legal framework provided by privacy and human rights law, CDRs are a commercial product that could be considered property. There is very little precedent for this type of adjudication, but the given degree of global data commercialization, there's little to suggest that CDRs wouldn't create a property rights interest. A more contentious question is whether that property rights interest exists for the mobile network operator, the customer, or both parties – and whether anonymization affects those rights. If a customer does have a property right in their data, mobile network operators would not have a legal right to share CDRs with third parties absent informed consent.

The Constitution of Liberia provides both for the inviolability of private property and for the expropriation authority of the Government.[105] Although originally intended for "real property," meaning land, the expropriation authority is applicable to the release of CDRs, but it imposes several additional requirements: (1) justification for the expropriation given to the owner; (2) prompt payment of just compensation; (3) the free right to challenge in a court; and (4) a reversion to the owner at the end of use.[106] In other words, Governmental expropriation of property is legally provided for, but subject to typical due process requirements. Liberia also has a Public Health Law, which extends the right of expropriation to include unused supplies, which could very easily be interpreted to apply to CDRs – provided that they were proven to useful to the emergency response effort.[107]

The application of expropriation requirements would significantly slow the process of releasing CDRs, as well as creating several difficult logistical challenges. It may be that expropriation justifications don't require measures of necessity or proportionality – but owners of the data could certainly challenge the validity of the data models employed or the availability of migration data through less invasive means. Even if the use of CDRs were determined to be necessary, that judgment then puts the court or the Government of Liberia into the unique position of assessing the independent value of CDRs data. Similarly, it is nearly impossible to enforce limitations in the use of raw data – especially data intended to be shared amongst a wider group of people – raising questions around the right of reversion or first refusal after the epidemic. For the purposes of this analysis, should the Government compel the release of CDRs, both mobile network operators and customers could bring suit against the Government for any failure to comply with the due process requirements involved.

104 Ibid.
105 The Constitution of the Republic of Liberia (1986) Article 20 and 24 available online http://www.tlcafrica.com/constitution-1986.htm.
106 The Constitution of the Republic of Liberia (1986) Article 24(a)(i-iv) available online http://www.tlcafrica.com/constitution-1986.htm.
107 Public Health Law (1976) Article 14 available online http://www.fahnbulleh.net/docs/lr_public_health_law.pdf.

Ultimately, the legal theories involved – whether privacy or property protections – hinge on questions of user consent or the application of due process in the extraordinary application of emergency powers. As demonstrated by the example of what actually happened, these theoretical and legal questions are less likely to determine the outcome than the practical structures in place to implement, oversee, and enforce the use of CDRs for the public good. In the throes of the Ebola epidemic, it's clear that there wasn't capacity to consider or the mechanisms to manage the significant data privacy, ownership, and licensing issues raised by the operational requirements of an increasingly digital disaster response community. Despite that, it is equally clear that understanding the enforcement systems for existing laws and privacy frameworks is a fundamentally important part of building a functional, digital disaster response ecosystem.

Chapter 6: The Law Inaction

Institutions and legal systems charged with protecting individual rights in digital spaces have been slow to adapt to evolving jurisprudence. The judicial bodies with the most relevant authority understaff regulatory agencies or international human rights enforcers, which most victims struggle to access. Even under the best of circumstances, resolving disputes that arise out of the large-scale use of sensitive data without user consent is complicated. The majority of cases to date have come from commercial breaches caused by the illegal exploitation of security vulnerabilities in digital systems.

The underlying issues become even more complicated when they involve government actions or complicity in sharing sensitive data with third parties in violation of its own law, without user consent. We don't have any sense for the size of emergency required to necessitate a government's use of digital emergency powers. Similarly, there are not established professional or data security standards for data protection that may provide protection against negligence actions – an issue raised by the recent hacking of the United States' Office of Personnel Management, which resulted in the exposure of the personally identifiable records of more than 19 million people. The issues involved are complex enough that they don't benefit from precedent in any specific jurisdiction, let alone usable examples in an international or emergency context. These issues get even more complicated during times of crisis, when a Government compels or is complicit in the use of potentially sensitive information to mitigate the effects of an international epidemic.

Lack of institutional capacity, legal precedent, or procedural clarity do not protect any of the organizations involved, nor are they a defense if an individual or group of people whose rights have been violated should choose to bring suit. These factors contribute to the uncertain and potential liability currently facing the governments, mobile network operators, and international organizations involved in international disaster response.

This Chapter examines the practical issues and legal mechanisms to resolve the disputes and lawsuits that could arise from the collection, use, or sharing of CDRs – or other personally identifiable information - during the Ebola response in Liberia.

Practical Issues

At a practical level, demonstrating harm from the aggregated release of data, especially data that has gone through anonymization and re-identification, is extremely difficult. The types of harms that could result are both difficult to predict and difficult to measure. For example, if data is released and then subsequently used to misallocate disaster response resources, it would be nearly impossible to prove to a legal standard that those resources would have otherwise been properly allocated. Similarly, if CDRs are maintained by a humanitarian organization and used for

commercial advantage in a subsequent procurement process that grants improper favor in a competitive process, it would be almost impossible for the original source of the data to know, let alone prove harm. Data is inherently difficult to track once released, as are the terms of the original license, prohibitions against international sharing, or determining the appropriate jurisdiction in which to bring suit. These are all issues that point to the need for an independent, proactive data management body, whose mandate enables them to determine the operational, commercial, and legal context for sharing sensitive information. That is not, however, to suggest that Data Protection Authorities are a comprehensive solution.

Fundamentally, creating an ethical and legal ecosystem that provides for informed consent, transparency, and meaningful user agency will require significant changes to commercial and public legal infrastructure. The following are four practical principles that should underpin any determination of the release of CDRs in future emergencies.

Consent

From a legal perspective, informed consent is the most powerful and pervasive tool to ensure the legality of information sharing. The principle appears in nearly every level of legal construction, beginning with commercial contracting and rising all the way to international human rights protections. The fundamental tension is that informed consent requires reasonable structures for limitation and enforcement. Looking, for example, at organ donor programs, broadly stated purposes and exemptions with strongly defined chains of custody and systems of management have created an essentially safe mechanism for people to share some of their most important property. Every person has the independent and legally legitimate right to share their information and there's no question that, faced with a global health pandemic, many people would voluntarily share information about themselves in order to improve the response effort.

Obtaining consent at point of collection is both a legal requirement in the Liberian context and a commercial practice that has significant precedent for less altruistic means. There is no question that building emergency data use clauses into commercial and public service contracts is both the most straightforward and the most legal way to facilitate the sharing of CDRs, and minimizes virtually every other question that the law compels.

Regulatory Validation

Data modeling is a fundamentally uncertain science, despite the tremendous gains it has the potential to add to our most vital systems. At present, though, our understanding of this process is so nascent that it raises a huge need for public and transparent validation processes before being employed in social and disaster engineering. Nearly every product brought to market that has the potential to affect public health, let alone emergency response, is subject to some degree of testing and regulation to ensure quality. This is typically done prior to use and in environments that graduate or mitigate risks through successive iterations. There are few good arguments that

data modeling should not be subject to the type of research and development testing that is applied to public institutions or resource allocation.

Absent validation, nearly every legal argument that enables the sharing of personal data fails, because there is no proof of benefit to counterbalance the very real costs involved. This isn't to suggest that there isn't value, rather that until it's proven and given character by independent and transparent processes, it will be subject to doubt, abuse, and significant legal challenges.

Necessity and Proportionality

Two of the most common challenges to a "public good" action are necessity and proportionality. Necessity is the idea that the action taken – in this case, the sharing of personally identifiable data without user consent – was necessary to achieve the desired goal. Necessity builds on the need for regulatory validation, because it explains the role that CDRs play in the overall model and also shows that there were not viable alternatives. In the case of the Ebola epidemic, responders alleged that real-time mobility information was necessary in order to optimize the allocation of response resources and contain the virus. Supporters of this thesis would rightfully point to the fact that this data simply doesn't exist in other formats and that the goal of containment is more than enough to justify the use of that data. Skeptics of this thesis would question whether real-time, aggregated migration data actually improves the understanding of the spread of a contact-based disease, whether the quality of the data could distort response efforts toward the digitally connected, and whether any of the involved institutions had the means to operationalize whatever insights might have emerged from the model. During the Ebola epidemic, the intentions of the organizations requesting data largely substituted for necessity justifications – which were often effective in securing data, but not in a way that provides any legal defense.

Proportionality is the principle of ensuring that the potential benefit of an action is proportional to the potential negative consequences of that same action. It seems like a straightforward balancing test, but it quickly becomes convoluted, particularly when neither the benefits nor consequences are known. Fundamentally, real-time pipelines into mobile network operator infrastructure are some of the most powerful data assets in the world, and there simply isn't much information about what governments, let alone international organizations, will do with that kind of access.

The early indications provided by intelligence agencies and public health authorities suggest at least the potential for the large-scale violation of basic freedoms. While it may seem melodramatic, Liberia has experienced two large civil wars in the last 25 years – and the potential for blurring humanitarian and national security justifications for data use has very high stakes. Proportionality as a principle fundamentally only works when there are clear values and processes to establish the value of CDR use to justify the use of real-time data infrastructure – which is different than recognizing the enormity of a threat. In the uncertainty and panic that arose from the Ebola epidemic, the international community recognized the potential threat of the outbreak, but there

was very little discussion around the proportionality of seizing CDRs. Similar to necessity, proportionality is not a bright line standard, but it is a balancing test that is often used to assess the legal validity of the actions of Governments and international actors during times of emergency.

Legal Mechanisms

The viability of legal enforcement mechanisms is, ultimately, the primary determining factor in whether our rights are protected by the laws we put in place. This analysis focuses on the available causes of action to a citizen of Liberia, who is a mobile network customer whose CDRs were shared with the Government. As mentioned above, depending on the particular actors in any specific fact pattern, there may be a wide range of additional legal mechanisms and venues available. CDRs that were shared with international organizations or transported across international borders, especially outside of ECOWAS member countries, would create additional causes of action before other courts.

One of the major challenges in bringing a suit, in addition to those stated above, is that it is extremely difficult to define an appropriate penalty or resolution. There aren't commercially established rates for CDR data, and certainly not ones that are likely to have significance at an individual level. In addition, privacy violations are difficult to quantify in terms of damages, so a litigant is likely to be left with speculative or punitive damages, which most courts are likely to be hesitant to levy against their own government.

Ultimately, there are four places that a Liberian citizen can go to seek redress: (1) customer service; (2) the LTA; (3) Liberian court; and (4) the ECOWAS CCJ. Although each could be escalated from one venue to the one after it, it's also possible to bring a case of first impression in each.

Customer Service

There are a number of pieces of Liberian telecommunications regulation that require mobile network operators to have dispute resolution processes, including the LTA 2007, the New Consumer Guidelines, and Consumer Bill of Rights.108 Though the mechanisms exist, it's not entirely clear what kind of liability a mobile network operator bears in complying with a Government order, or what kind of redress they could offer. The best-fit causes of action against a mobile network operator would likely emanate from the way they collect, use, and maintain data – or, if a litigant could prove it, the sharing of data with a third party organization absent government influence. That said, Customer Service would be a disadvantageous venue in which to bring a serious case. An optimistic outcome would be an improvement in Terms of Service Agreements or overall transparency in data practices.

Liberian Telecommunications Authority

The LTA 2007 and supporting legislation gives the LTA a broad authority to hear and adjudicate disputes between customers and service providers, including a relatively granular structure for complaint submission and processing.109 The LTA has the broadest available authority in relation to punishing mobile network operators, and can do anything from levying fines to imposing injunctive relief to removing the license altogether. Although the LTA requires good faith negotiation between parties in advance of being willing to hear most cases, it is also able to issue binding opinions. The authority of the LTA, understandably, doesn't reach to being able to sanction the Government for telecommunications-related violations of human rights. If a customer is challenging such an action, they are likely challenging the LTA, so are best served in a more neutral venue.

The LTA is an ideal venue, however, to challenge mobile network operator Terms of Service Agreement standards, the legality of their data collection, and any provable sharing of CDRs with third parties. Similarly, the LTA would likely have at least an advisory role in determining whether CDRs qualified as property, related to questions around the validity of expropriation claims.

Liberian Courts

Liberia's court system is a microcosm of a wide range of institutional challenges, in a country beset by a significant amount of instability in the last few decades. Liberian courts have received significant criticism for their treatment of prisoners, human rights, and due process. As compared to other regional court systems, Liberia does well in limiting government powers and ensuring fundamental rights, which bodes well for potential litigants.110 It fares far less well in regulatory enforcement, civil justice, and corruption indicators – all of which would be materially involved in any case brought against a mobile network operator or the Government related to the use of CDRs during the Ebola outbreak.111 Although a Liberian mobile network customer could bring almost any of the available causes of action to a Liberian court, like most civil systems, the available remedies are primarily financial. Similarly, although the ECOWAS Supplementary Act was ratified by Liberia, there isn't much precedent to suggest an obvious outcome or available redress.

ECOWAS Community Court of Justice

The CCJ determines admissibility of cases, although it specifically does hear human rights cases of individuals against their government. In addition, the CCJ has a wide range of available remedies, including the ability to compel a government to change a practice or fulfill an obligation under ECOWAS law. As a result, CCJ won't hear an individual's case against a mobile network operator – but would be able to adjudicate violations of privacy and, potentially, the validity of due process implementations of an expropriation process.

In the case of the Ebola epidemic, any theory of expropriation would likely need a more tangible

fact pattern to justify a due process case. However, given the state of the Liberia's implementation of its Data Protection Authority – and the availability of ECOWAS as an adjudicator of specific issues arising from the Supplementary Act – there's a solid likelihood that the CCJ could compel both punitive damages for privacy violations and investment in the institutional infrastructure to guide future seizures or requests for CDRs.

Conclusion

The international digitization of disaster response raises a range of urgent issues that need attention, coordination, and action from every group involved. Although these issues are complex, the current state of digital coordination, human rights protections, and disaster experimentation create significant harm for the world's most vulnerable people and significant liability for some of the world's best organizations. Defining the digital exercise of emergency powers, regulating the experimental application of data models in humanitarian settings, and protecting the rights of vulnerable populations during times of crisis are some of the most important issues of modern humanitarianism–and there won't be easy answers. What there will be, in the meantime, is the risk that these issues will get settled through courtrooms instead of consultative and participatory processes. The thing no organization operating in a fragile or international context can do anymore, is ignore the practical, technological, and legal steps necessary to build digital systems that truly do no harm.

The Ebola epidemic in West Africa was one of the worst health crises in modern history, and it exposed a wide range of traditional and emergent issues in the way that international organizations, governments, and commercial organizations manage the growing digitization of disaster response. The public health infrastructure in Liberia was unprepared for, and incapable of containing, the outbreak of the Ebola virus. The international response was dangerously slow, and when it intervened, it initially compounded communication challenges.

The failure to communicate became the characterizing narrative of the outbreak and rather than focus on centralizing coordination, a large number of actors intervened. Coordination runs counter to most people's instincts in disaster and takes time, which is in short supply – particularly when the death toll is rising. Hundreds of individuals, donors, governments, and response organizations mobilized, pouring disembodied information systems, resources, and people into an already chaotic operational context. Each effort, though, ultimately needed either institutional response or operational capacity to have impact – straining Liberia's already overwhelmed management and coordination infrastructure. Within that context, response efforts factionalized and regionalized in an effort to manage the signal-to-noise ratio. The result was patchwork reporting, incompatible information infrastructure, disconnected operational efforts, and significant tension with the Government of Liberia.

Rather than focus on building integrated coordination systems, the calls from the international community pushed for an increase in the availability of data – under the presumption that open and interoperable data systems could improve response capacity. Universal availability of information, while a potential improvement, does nothing to harmonize disparate definitions, assign administrative permissions, or attribute comparative reliability. These core needs are the

foundations of functionally scalable information architecture – but they are not primarily technology problems, they are coordination problems. To that end, pushing for decentralized information systems has the potential to undermine the ability of central actors to coordinate and manage operations.

The request for CDRs, the most invasive request for data, challenged more than good practice in humanitarian response, it pushed for expropriation of direct access to some of the most sensitive databases in the world. Although there are interim states of anonymization of that data that could mitigate some of the risk to its subjects, the data models it would be used in are still extremely experimental. In addition, nearly every described use of CDRs requires some form of re-identification or correlation with datasets that fall under the definition of "personally identifiable," triggering a wide range of privacy laws and risks. Although a number of the requests made recognize the implications and complications posed by the release of CDR data, very few acknowledge existing data protection laws or the experimental nature of the justification for the expropriation of personal information.

Although this is not the first time that disaster response operations have been used to justify investment in untested approaches, it is one of the most invasive. Unlike many other forms of experimentation that happen during emergency responses, data lasts forever. It is also almost impossible to track or control once released. Not only is it premature to ascribe value to the abrogation of the privacy of millions of people, it's impossible to how far or for how long those datasets may pose a risk to the people they identify. There simply aren't yet strong enough global technological, operational, organizational, legal, or economic mechanisms in place to measure the benefits or manage the risks involved.

The laws that do exist to govern this type of data request suggest that this kind of expropriation, undertaken without any form of due process, would be illegal. Given the novelty of the request, there's no precedent for this type of data seizure, nor is there any certainty that the available enforcement mechanisms have the capacity or the requisite independence to evaluate the costs or benefits of such a practice. What is certain is the growing interest and willingness of a wide range of actors to take advantage of these datasets during the periods of panic surrounding emergency – often in ways that limit fundamental freedoms with the threat of force.

As so often happens when confronted with potential – especially in emergency – the international community underestimated the present and future risks of using CDRs and data modeling to guide disaster response. There is little question that the use of appropriate data to feed the operations of a well-coordinated response effort has significant potential to reduce human suffering. But that potential is far from realized, and if we're going to realize it, we'll need to build the institutional coordination, mathematical validation, and legal rights frameworks so that the benefits of digitization evolve alongside our ability to control them.

The response to the Ebola epidemic raised a wide range of important issues in modern disaster response, but it didn't acknowledge or respect the rights of the people it meant to serve. For that reason, West Africa's Ebola epidemic – and Liberia's experience with it – was a big data disaster.

Recommendations

In order to build a supportive and safe space in which to design, test, and implement strong data modeling frameworks for social engineering and disaster response, there will need to be engagement at a range of levels. The following are a top-level series or recommendations, though they are by no means comprehensive:

International Organizations

1. Invest in transparent and publicly accessible experimentation infrastructure for data modeling applied to social issues or circumstances. Determine appropriateness criteria based on relevance, risk, and confidence thresholds. Create public engagement systems around the governance of these models.

2. Treat information architecture like treaties, proposing globally usable systems and structures, which are ratified, approved, and implemented at the national level. Publicly document variations based on local infrastructure.

3. Require regular reporting to local institutions as an indicator of compliance and impact, with set thresholds as requirements for the release of follow-on funding or eligibility for subsequent awards.

4. Include standard indicator definitions and technological interoperability as a procurement requirement for humanitarian response organizations. Ideally, these would be coordinated between donors and universally applied.

National Governments

5. Establish public information data licensing templates, including purpose requirements, use limitations, and enforcement frameworks. Keep records of adherence and use good faith as a determining factor of future access.

6. Establish clearer intermediary liability and emergency power doctrines, as applied to digital information. Also build clearer frameworks to establish the limits, gradients, and independent review of emergency authority renewals.

7. Implement EU and ECOWAS “style” Data Protection Authorities, with proactive enforcement mandates and powers.

Commercial and Digital Service Providers

8. Explicitly include data licensing terms in agreements with end users, including dispute resolution clauses, emergency circumstance requirements, and remedies in case of violation.

9. Include an opt-in “data donor,” program that enables users to proactively contribute their data to selected research institutions, charities, and/or emergency response organizations.

10. Build relationships with international human rights enforcement bodies, in order to be able trigger or report third party abuses.