

Ethical Considerations for Movement Mapping to Identify Disease Transmission Hotspots

Bouke C. de Jong, Badou M. Gaye, Jeroen Luyten, Bart van Buitenen, Emmanuel André, Conor J. Meehan, Cian O'Siochain, Kristyna Tomsu, Jérôme Urbain, Koen Peeters Grietens, Maureen Njue, Wim Pinxten, Florian Gehre, Ousman Nyan, Anne Buvé, Anna Roca, Raffaella Ravinetto, Martin Antonio

Traditional public health methods for detecting infectious disease transmission, such as contact tracing and molecular epidemiology, are time-consuming and costly. Information and communication technologies, such as global positioning systems, smartphones, and mobile phones, offer opportunities for novel approaches to identifying transmission hotspots. However, mapping the movements of potentially infected persons comes with ethical challenges. During an interdisciplinary meeting of researchers, ethicists, data security specialists, information and communication technology experts, epidemiologists, microbiologists, and others, we arrived at suggestions to mitigate the ethical concerns of movement mapping. These suggestions include a template Data Protection Impact Assessment that follows European Union General Data Protection Regulations.

Human and pathogen co-evolution has led to a vast array of transmission routes, transmission dynamics, and risks for infection. Human behavior, particularly movement between locations, plays a primary role in the transmission dynamics of infectious diseases (1). Geospatial areas with high prevalence or efficient transmission of disease are known as hotspots (2). Transmission hotspots can be thought of as nodes in space and time where the density of contact

between infected and uninfected persons is higher than average, increasing the risk for disease transmission.

Interrupting transmission is key to preventing and controlling infectious diseases (1). Timely identification of transmission routes and hotspots is necessary for tailoring public health interventions. However, many interventions that effectively break transmission chains also invade the private sphere of affected persons or communities and often are at odds with personal liberties (3). Some methods of identifying transmission hotspots could reveal sensitive information on behavior and the inner functioning of a community, making these methods problematic from an ethics point of view.

Traditional public health approaches to mapping human-to-human transmission routes include contact tracing and molecular epidemiology. Both approaches are laborious, costly, and limited. Contact tracing, in which investigators follow up with named contacts to identify those at risk for exposure (4), lacks sensitivity for population-based interruption of transmission chains. Molecular epidemiology uses genetic typing of pathogens isolated from patients to trace transmission by highlighting genetic similarity (5) but is prone to undersampling, potentially missing key events in complex transmission chains. Because of laboratory delays, molecular epidemiology frequently does not lead to actionable findings. In addition, this method is not feasible outside of research institutions in many low- and middle-income countries, where higher rates of infectious diseases occur.

A promising alternative to contact tracing is to identify transmission hotspots where public health workers can tailor preventive strategies. During an infectious disease outbreak, as control increases in the general population, the disease typically spreads heterogeneously. Transmission events then concentrate in areas and communities not reached by conventional approaches.

When the goal is elimination and ultimate eradication of a specific disease, tackling transmission hotspots is key. Information and communication technology (ICT), such as global positioning systems (GPS), smartphones, and mobile phones, could provide a novel approach to

Author affiliations: Institute of Tropical Medicine, Antwerp, Belgium (B.C. de Jong, C.J. Meehan, K. Grietens, M. Njue, F. Gehre, A. Buvé, R. Ravinetto); Medical Research Council Unit, The Gambia at London School of Hygiene & Tropical Medicine, Fajara, The Gambia (B.M. Gaye, C. O'Siochain, F. Gehre, A. Roca, M. Antonio); Katholieke Universiteit Leuven, Leuven, Belgium (J. Luyten, E. André); White Wire Data Protection, Kontich, Belgium (B. van Buitenen); Dalberg Data Insights, Brussels, Belgium (K. Tomsu, J. Urbain); School of Tropical Medicine and Global Health, Nagasaki University, Nagasaki, Japan, and Amsterdam Institute for Social Science Research, Amsterdam, the Netherlands (K. Grietens); Hasselt University, Hasselt, Belgium (W. Pinxten); Bernhard Nocht Institute for Tropical Medicine, Hamburg, Germany (F. Gehre); University of The Gambia, Serrekunda, The Gambia (O. Nyan)

DOI: <https://doi.org/10.3201/eid2507.181421>

identifying transmission hotspots (Appendix 1, <http://wwwnc.cdc.gov/EID/article/25/7/18-1421-App1.pdf>). One promising approach is to map movements of persons by using ICT data to identify behavior patterns and transmission hotspots where cost-effective prevention strategies could be implemented. This type of mapping could reduce transmission of diseases that are difficult to eliminate, such as tuberculosis (TB), leprosy, schistosomiasis, malaria (6), and sleeping sickness, and assist in controlling outbreaks of acute disease, such as Ebola virus (7,8), cholera, or Shiga toxin-producing *Escherichia coli* O157:H7 (9). However, mapping the movements of potentially infected persons comes with many ethical challenges.

We proposed a project in which researchers request informed consent from TB patients to map their aggregate movements through their cellular phone call detail records (CDRs). In the context of this project, we convened a 1-day meeting on the ethical aspects around the use of mobility data for mapping infectious disease transmission. The meeting, held October 24, 2017, at the Institute of Tropical Medicine (Antwerp, Belgium), included researchers, ethicists, data security specialists, ICT experts, epidemiologists, microbiologists, and a representative from a national TB program (Appendix 2, <http://wwwnc.cdc.gov/EID/article/25/7/18-1421-App2.pdf>). The objective for the 20 participants was to consider risks and benefits of using ICT data to map movements of infected persons and identify transmission hotspots of TB and other infectious diseases. From this meeting, we developed a model Data Protection Impact Assessment (DPIA) template that others can use to conduct a similar assessment (Appendix 3, <http://wwwnc.cdc.gov/EID/article/25/7/18-1421-App3.pdf>). We focused mainly on ethical aspects for research but also addressed specific concerns that could arise if the approach is scaled up for programmatic use.

Data Sources for Detecting Transmission Hotspots

Information on case mobility, typically collected by public health officials or researchers through patient interviews,

is crucial for tracking pathogen transmissions. However, the limited population sample interviewed introduces selection bias. In addition, questionnaire data on mobility might lack sufficient detail and are prone to both recall and information bias. Because of the complexity and cost, interviews and questionnaires are difficult to implement in programmatic conditions and do not allow for real-time interpretation using autonomous self-learning algorithms.

The global penetration of mobile phones could provide a viable means to track infectious diseases by electronically mapping case mobility data. Worldwide, 66% of the population used mobile phones in 2017, counting unique mobile subscribers and corrected for use of multiple subscriber identification module (SIM) cards. Of global SIM cards, 57% are used in smartphones, without correcting for multiple SIM card users (10). We discussed 3 options for collecting ICT data: a dedicated smartphone application, a separate GPS tracking device, and mobile phone call records (Table; Appendix 1).

Ethical Issues of Mobility Mapping

Collecting mobility data linked to health information poses specific challenges for upholding ethics principles described in basic guidelines for human subjects research. We see 2 highly relevant ethical obstacles: protecting the participants' privacy in relation to principles of autonomy and nonmaleficence and finding a balance between costs, risks, and benefits for participants and communities in relation to principles of beneficence and justice (11).

Protecting Participants' Privacy

The European Union General Data Protection Regulation (EU GDPR, EU Regulation 2016/679) (12) and Guideline 22 of the Council for International Organizations of Medical Sciences (13), among other regulations, explicitly stress the need for protecting the privacy and confidentiality of persons and their information. In all situations, investigators must put protective measures in place to avoid breaches in confidential mobility data that might cause unintended inferences about a user's life (14).

Table. Characteristics of different approaches to collecting mobility data for mapping infectious disease outbreaks*

Characteristics	Source of mobility data		
	Dedicated smartphone application	GPS tracker	Call detail records
Scalability to large populations	Medium	Low	High
Retrospective analysis possible	Likely, depending on stored location data on phone at time of installation	No	Likely, depending on duration of data storage at telecom operators
Spatial resolution	High, depending on mobile data use and WiFi density	High	Variable, depending on cell tower and mast density
Participant control	Medium	High	Low
Third party access to private information	Possibly	Unlikely	Likely
Need for uninfected controls	Possibly	Unlikely	Likely, to avoid identification of health information by telecom operators

*GPS, global positioning system.

Outbreaks of highly infectious diseases, such as Ebola and cholera, along with endemic diseases, such as HIV and TB, are more prevalent in low-income countries. Many mobility tracking approaches have been implemented to identify infectious disease hotspots in these areas (6,15–19). In international collaborations, researchers from abroad should apply the same ethics and regulatory standards they would apply in their own countries. EU-funded researchers working outside the EU must ensure their research adheres to EU GDPR standards. Mapping across national boundaries might require further ethics and data security safeguards and the perceived balance between benefit and risk of mapping mobility might be different in diverse social and cultural contexts.

In some circumstances, investigators might have difficulty meeting ethics requirements for informed consent. Waivers for informed consent can be granted by the concerned ethics committees, but only under exceptional circumstances; for instance, during outbreaks, if the research is low-risk and has potential for high societal value; if obtaining written consent is unpractical or unfeasible; and if data anonymization and other adequate measures are in place to mitigate confidentiality and privacy risks.

Linking health conditions or diagnoses with patient movements constitutes a high risk to infected persons. Consequently, investigators should not have access to the movements of individual patients, and telecommunications staff should not be able to link movements of persons with their health-related information. Participants should be aware of these risks when asked for their telephone data. They also should be informed of their right to refuse or withdraw their consent for use of their data.

The challenges are even greater for mapping movements of children. Most children do not routinely keep mobile phones; great cultural and socioeconomic variations exist in the age of first phone use and in adult supervision. Children under a certain age presumably would be accompanied by adults. Just as in other kinds of research, minors should be asked for assent when their parent or guardian is asked for informed consent, according to their capacity and maturity, while adhering to local regulatory requirements. Additional ethics challenges might arise if parents or guardians request access to the mobility data of their children.

Costs, Risks, and Benefits for Participants and Communities

In public health ethics, the dilemma of individual risk versus population benefit is well-recognized (20,21). When weighing risks to participants' privacy against potential population benefits, researchers must consider the participants' status. Patients, contacts of patients, or healthy persons sampled from the general population

will have different risks to their privacy or benefits for their communities.

Study participants will not directly benefit from knowing where they might have acquired or spread an infectious disease. Therefore, the realistic potential of a study to contribute to improved public health must be considerable to outweigh the risk to the participant. Spatiotemporal analysis of data can show where infected persons crossed paths when they were infectious but is not proof of actual transmission events. These data can indicate locations where the density of infected persons was higher and might point to previously unsuspected transmission hotspots.

Communities or neighborhoods with confirmed or suspected infectious disease transmission hotspots might be stigmatized. Such stigma could have further negative consequences, such as discrimination against groups or neighborhoods, reduced tourism (22), or decreased property values. Although anonymized data can focus on neighborhoods rather than specific buildings, stigma could occur at businesses, schools, social venues, or healthcare facilities in an area identified as a transmission hotspot. Researchers should consider such risks and plan adequate mitigating measures during protocol development and should include representatives from involved communities during protocol development. Community representatives can provide a firsthand understanding of local challenges, such as the community's perception of the disease; whether specific persons are typically stigmatized in the community; whether persons could be legally prosecuted for behaviors associated with disease transmission, such as drug use or same sex intercourse in some areas; and how to provide information back to the community. Researchers should not presume that they can identify representative community leaders. In some contexts, leaders are obvious, such as patients with HIV or TB who are active in local associations, but identifying these leaders might be more difficult in urban settings or in disrupted communities under the stress of an outbreak.

In contrast to the ethical risks, researchers also should consider whether withholding the vast amount of mobility data would be unethical and whether an ethical imperative exists to use the available data for maximal benefit (23). Ultimately, if residual risk is acceptable, analysis of mobility data can be justified if it can yield actionable insights that benefit public health.

Researchers also should consider whether, and how, to communicate information on hotspots to the general population. In doing so, they must question whether public health interventions in the hotspots are sufficient to reduce the risk for infection for persons moving into and out of those areas. If so, avoiding communication about specific hotspots could reduce the chance for stigma in that community. On the other hand, if persons moving into or out of

hotspots need to take protective measures, such as wearing a mask or avoiding the area altogether, then researchers should put the utmost care into communicating appropriate messages.

Mitigating Ethical Challenges

During the protocol design phase, researchers should assess the risk-benefit balance of their intended movement mapping strategy, address risks for privacy breaches, and plan for mitigating such breaches. The Global System for Mobile Communications Association and others have developed guidelines and outlined ethical challenges for using telecommunication data (24–27). However, no single framework will fit the myriad of movement mapping approaches or all applications for the identification of transmission hotspots of infectious diseases.

According to the EU GDPR, personal data can only be processed under specific circumstances for a well-defined and communicated purpose, and only when participants consent and data processing is proportionate to the purpose (12). Personal data cannot be processed beyond what is known or expected by the research participant and cannot be kept longer than needed.

A DPIA provides a framework to mitigate risks by taking privacy principles into account in the earliest conception and engineering phases of a project or data processing application (Appendix 3). Along with an analysis of residual risks, researchers should conduct a DPIA before beginning data collection.

Involving Communities as Research Stakeholders

Including the community and its members as stakeholders during the design phase will help investigators convey the public health benefits of the project and minimize misunderstanding, mistrust, and panic. To maintain accountability to communities, researchers should involve them in the preparation, implementation, and evaluation of aggregate movement mapping data. By working with community members, investigators can address concerns about risks and benefits to the community and its members.

Potential approaches to enhancing community input include involving community advisory boards or similar community structures in the study protocol design (28,29); carrying out a preliminary qualitative study to investigate the perception of local policy makers and members of the community about the mobility data collection; or carrying out a rapid ethics assessment, a brief qualitative intervention used to examine the ethics terrain of a research setting before recruiting participants (30). Such participatory research approaches engage communities in the research process and take local perception into account during research planning (29).

To further reduce the chance of stigmatization of the neighborhoods or groups, researchers should install measures to prevent identification of transmission hotspot locations by outside parties. Such measures could include confidentiality agreements with local public health authorities and communication plans to reduce the consequences of misuse of information by the media or other actors.

Aggregating Data

Researchers should use aggregate analyses of mobility data to reduce the risk of breaching participants' privacy and confidentiality (24,25). This process could involve anonymizing phone numbers associated with CDRs so that patient information can be viewed without revealing identities or phone numbers of participants. In addition, researchers can use algorithms that permit aggregate analysis of a minimum number of participants' CDRs to reduce the chance of pinpointing a participant's movements. Aggregate CDRs provide background mobility controls, while still calculating relative risks of transmission hotspots. In the absence of aggregate CDRs, investigators can still identify hotspots with few relative risks to participants' privacy.

Requesting Informed Consent

Informed consent and patient information sheets should be transparent, specific, and unambiguous. The aim is to guide participants' understanding of the project's purpose, as well as how investigators will handle their personal data, protect their confidentiality, and address any residual risks to personal information after the study. During the consent interview or in the consent documentation, researchers should reduce jargon and present information in plain language appropriate for the audience. Investigators also might use teach-back methods, back translation, and pilot testing with the target group to assist in developing accurate informed consent and patient information sheets.

Participants should be informed how long their data will be stored before destruction and the deadline by which they can request rectification or destruction of their data. A rapid ethics assessment also can help improve the design of the informed consent tools for a given population. Study personnel should be properly trained on the informed consent and data collection procedures.

Considerations for Telecommunications Regulatory Authorities and Providers

In addition to ethics approvals, the telecommunication regulatory authorities must approve use of CDRs and mobile phone companies will require confidentiality and data transfer agreements. Researchers will need to ensure that mobile network operators and their employees comply with the same confidentiality rules applied in the health sector,

including securely handling, storing, and limiting access to data. Agreements with mobile phone companies should specify that they not share data with other parties or retain it longer than necessary.

One way to minimize the chance for mobile network employees or others to link CDRs to a particular disease profile is through recruiting uninfected participants as control cases. Researchers can include uninfected participants' CDRs, with their consent, from the same catchment area as the patients. Control participants benefit public health without gaining a personal benefit, but they face the same risk for confidentiality breaches. In addition, such breaches could cause them to be mistaken as infected with the disease. No clear precedent exists to help set a dilution rate (i.e., the ratio of uninfected controls to patients) to sufficiently mitigate the chances of linking a person with an infectious disease diagnosis. However, more controls might favorably shift the risk-benefit balance.

For data analysis, researchers should use algorithms that prevent disaggregation of data and reduce opportunities to link health information and mobility patterns with any participant's identity. After aggregating the analysis, investigators can filter out controls to arrive at hotspot information.

Communicating Information on Transmission Hotspots

When researchers publish study findings, they should clearly demonstrate that they followed all ethics rules and discussed a response plan with local communities and public health authorities, especially when they discuss a previously unknown public health problem in a specific community. To avoid revealing exact locations, researchers can include graphical representations rather than recognizable maps. Researchers also can request to override any requirements for sharing the full or aggregated dataset and associated metadata at the time of publication due to privacy concerns.

Regardless of safeguards, the media, authorities, or politicians could misuse published results or take the findings out of context. Although a data transfer agreement with a mobile network will not prevent misuse of information, researchers can reduce negative consequences of such misuse by developing a comprehensive communication plan with community stakeholders and public health authorities before starting the project.

Researchers should have an adequate understanding of the mobile technologies and related ethics requirements for each specific research project. Ethics committees might lack the knowledge and expertise to assess these protocols correctly and researchers should be prepared to explain the technologies and how they can benefit public health. In addition, ethics committees and institutional review boards should consider involving data

security specialists as more research begins to incorporate mobile technologies.

Implementing Mobile Mapping

After a research project demonstrates the feasibility of ethically using CDRs for identifying transmission hotspots, a national control program might choose to implement it. For a TB program, patients with confirmed TB could provide informed consent to release their CDRs to map their movements. Staff from the national TB program could periodically perform an aggregate analysis of recent CDRs to identify locations where transmission might have occurred.

In addition to ethics issues tackled during research, public health programs could encounter more ethics complexities. For instance, patients might experience a therapeutic misconception and feel obliged to consent to releasing their CDRs if the request comes from the same physician who is providing healthcare because they fear care will be withheld if they do not consent. Also, programs should be aware that routine surveillance data could be used for retrospective research, blurring the boundary between surveillance and research. Even if such surveillance is not intended as research, a public health program should involve the appropriate ethics committee. The ethics committee can assess the protocol for collecting mobility data and the informed consent tool, as well as the proposed project's public engagement and transparency plans to determine its benefit to the public (31).

Conclusions

With their unprecedented global penetration, mobile phones can yield vast amounts of information that offer opportunities for mapping infectious disease hotspots but also pose ethical challenges. We offer suggestions on safeguards to ensure data can be used to benefit public health while protecting the users' privacy and confidentiality. The EU GDPR protects EU residents and participants in EU-funded research in countries outside of the EU from abuse of personal information. The higher standards for the EU GDPR also apply to the ethics framework for research on mobility patterns conducted for public health benefits. By upholding these ethics standards, public health investigators could use mobility mapping to identify infectious disease transmission hotspots without compromising the privacy of patients or creating mistrust in communities affected by infectious diseases.

Acknowledgments

We thank Marianne van der Sande and Julie Vanvolsem for helpful discussions during the workshop on which this manuscript is based. The findings have not been presented elsewhere.

This work was supported by the European Research Council Proof of Concept “Enhanced Place Finding” (grant no. 727695).

About the Author

Dr. de Jong is a research scientist at the Institute of Tropical Medicine, Antwerp, Belgium. His research interests are clinical infectious diseases, epidemiology and tuberculosis transmission.

References

- Anderson RM, May RM. Infectious diseases of humans: dynamics and control. Oxford: Oxford University Press; 1991.
- Lessler J, Azman AS, McKay HS, Moore SM. What is a hotspot anyway? *Am J Trop Med Hyg.* 2017;96:1270–3. <http://dx.doi.org/10.4269/ajtmh.16-0427>
- Selgelid MJ, Battin MP, Smith CB, eds. Ethics and infectious disease. Malden (MA): Wiley-Blackwell; 2006.
- Koo D, Thacker SB. In Snow’s footsteps: Commentary on shoe-leather and applied epidemiology. *Am J Epidemiol.* 2010;172:737–9. <http://dx.doi.org/10.1093/aje/kwq252>
- Foxman B, Riley L. Molecular epidemiology: focus on infection. *Am J Epidemiol.* 2001;153:1135–41. <http://dx.doi.org/10.1093/aje/153.12.1135>
- Tatem AJ, Huang Z, Narib C, Kumar U, Kandula D, Pindolia DK, et al. Integrating rapid risk mapping and mobile phone call record data for strategic malaria elimination planning. *Malar J.* 2014;13:52. <http://dx.doi.org/10.1186/1475-2875-13-52>
- Tracey LE, Regan AK, Armstrong PK, Dowse GK, Effler PV. Ebola Tracks: an automated SMS system for monitoring persons potentially exposed to Ebola virus disease. *Euro Surveill.* 2015;20:20999. <http://dx.doi.org/10.2807/1560-7917.ES2015.20.1.20999>
- Peak CM, Wesolowski A, Zu Erbach-Schoenberg E, Tatem AJ, Wetter E, Lu X, et al. Population mobility reductions associated with travel restrictions during the Ebola epidemic in Sierra Leone: use of mobile phone data. *Int J Epidemiol.* 2018;47:1562–70. <http://dx.doi.org/10.1093/ije/dyy095>
- Chunara R, Freifeld CC, Brownstein JS. New technologies for reporting real-time emergent infections. *Parasitology.* 2012;139:1843–51. <http://dx.doi.org/10.1017/S0031182012000923>
- GSM Association. The mobile economy 2018. London: GMSA; 2018 [cited 2019 Feb 07]. <https://www.gsma.com/mobile-economy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf>
- The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont Report: ethical principles and guidelines for the protection of human subjects of research. Pub. no. 78-0012. Bethesda (MD): The Commission; 1979.
- European Union General Data Protection Regulation (GDPR). Frequently asked questions about GDPR [cited 2019 Feb 7]. <https://www.eugdpr.org/gdpr-faqs.html>
- Council for International Organizations of Medical Sciences (CIOMS). International ethical guidelines for health-related research involving humans. 4th edition. Geneva: The Council; 2016.
- Mittelstadt B. Designing the health-related internet of things: ethical principles and guidelines. *Information.* 2017;8(3). <http://dx.doi.org/10.3390/info8030077>
- Wesolowski A, Eagle N, Noor AM, Snow RW, Buckee CO. The impact of biases in mobile phone ownership on estimates of human mobility. *J R Soc Interface.* 2013;10:20120986. <http://dx.doi.org/10.1098/rsif.2012.0986>
- Wesolowski A, Stresman G, Eagle N, Stevenson J, Owaga C, Marube E, et al. Quantifying travel behavior for infectious disease research: a comparison of data from surveys and mobile phones. *Sci Rep.* 2014;4:5678. <http://dx.doi.org/10.1038/srep05678>
- Wesolowski A, Qureshi T, Boni MF, Sundsøy PR, Johansson MA, Rasheed SB, et al. Impact of human mobility on the emergence of dengue epidemics in Pakistan. *Proc Natl Acad Sci U S A.* 2015;112:11887–92. <http://dx.doi.org/10.1073/pnas.1504964112>
- Bengtsson L, Gaudart J, Lu X, Moore S, Wetter E, Sallah K, et al. Using mobile phone data to predict the spatial spread of cholera. *Sci Rep.* 2015;5:8923. <http://dx.doi.org/10.1038/srep08923>
- Wesolowski A, Eagle N, Tatem AJ, Smith DL, Noor AM, Snow RW, et al. Quantifying the impact of human mobility on malaria. *Science.* 2012;338:267–70. <http://dx.doi.org/10.1126/science.1223467>
- World Health Organization. WHO guidelines on ethical issues in public health surveillance. Geneva: The Organization; 2017.
- Kass NE. An ethics framework for public health. *Am J Public Health.* 2001;91:1776–82. <http://dx.doi.org/10.2105/AJPH.91.11.1776>
- Denecke K. An ethical assessment model for digital disease detection technologies. *Life Sci Soc Policy.* 2017;13:16. <http://dx.doi.org/10.1186/s40504-017-0062-x>
- Banaszek A. Tracking infectious diseases in cyberspace. *CMAJ.* 2011;183:E373–4. <http://dx.doi.org/10.1503/cmaj.109-3829>
- GSM Association. Guidelines on the protection of privacy in the use of mobile phone data for responding to the Ebola outbreak. London: The Association; 2014 [cited 2019 Feb 07]. <https://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>
- GSM Association. Mobile privacy and big data analytics. London: The Association; 2017 [cited 2019 Feb 07]. https://www.gsma.com/publicpolicy/wp-content/uploads/2017/02/GSMA-Big-Data-Analytics_Feb-2017.pdf
- de Montjoye YA, Hidalgo CA, Verleysen M, Blondel VD. Unique in the crowd: the privacy bounds of human mobility. *Sci Rep.* 2013;3:1376. <http://dx.doi.org/10.1038/srep01376>
- Taylor L. No place to hide? The ethics and analytics of tracking mobility using mobile phone data. *Environment and Planning D: Society and Space.* 2016;34:319–336. <https://doi.org/10.1177/0263775815608851>
- Marsh V, Kamuya D, Rowa Y, Gikonyo C, Molyneux S. Beginning community engagement at a busy biomedical research programme: experiences from the KEMRI CGMRC–Wellcome Trust Research Programme, Kilifi, Kenya. *Soc Sci Med.* 2008;67:721–33. <http://dx.doi.org/10.1016/j.socscimed.2008.02.007>
- Tindana PO, Singh JA, Tracy CS, Upshur RE, Daar AS, Singer PA, et al. Grand challenges in global health: community engagement in research in developing countries. *PLoS Med.* 2007;4:e273. <http://dx.doi.org/10.1371/journal.pmed.0040273>
- Negussie H, Addissie T, Addissie A, Davey G. Preparing for and executing a randomised controlled trial of podocinosis treatment in northern Ethiopia: the utility of rapid ethical assessment. *PLoS Negl Trop Dis.* 2016;10:e0004531. <http://dx.doi.org/10.1371/journal.pntd.0004531>
- Ballantyne A, Schaefer GO. Consent and the ethical duty to participate in health data research. *J Med Ethics.* 2018;44:392–6. <http://dx.doi.org/10.1136/medethics-2017-104550>

Address for correspondence: Bouke C. de Jong, Institute of Tropical Medicine, Nationalestraat 155, 2000 Antwerp, Belgium; email: bdejong@itg.be

Ethical Considerations for Movement Mapping to Identify Disease Transmission Hotspots

Appendix 1

Overview of mapping approaches, including information on smartphones, global positioning system (GPS) trackers, and call detail records

Smartphones

Smartphones can either be equipped with an application that tracks global positioning system (GPS) signals or requests permission to retrospective mobility data already gathered by other currently installed apps. An alternative is Google Location History, which is passively gathered on Android phones over long periods of time and has an accuracy similar to GPS in the UK (1,2). The advantage is that detailed movement signals will be available. The downside of this approach is that smartphone use, especially in low-income countries, is strongly associated with socio-economic status, limiting participation of the poorer patients mostly affected by infectious diseases (3–5). Also, the common practice of sharing a phone can limit the accuracy of data collected in such contexts. In low-endemic, high-income countries, such as those in the EU, due to greater smartphone penetration, this approach is likely more feasible and informative than the use of CDRs. However, poverty might again limit smartphone use in those at highest risk for certain infectious diseases.

Global Positioning System (GPS) Trackers

Alternatively, a participant can be asked to carry a GPS tracker during a certain period. Different designs are available that can be easily carried and will record the study participant's position every few minutes. Moreover, unlike in the case of smart phones, GPS trackers give strong control over access to the data, which minimizes the confidentiality and privacy risks to the participant, simply by leaving the device at home when they do not wish to be tracked. Disadvantages of handing GPS trackers to patients with a diagnosed infection include the

assumption that the prospectively collected movements are not modified according to the illness, diagnosis, or treatment. Especially in the presence of an ongoing outbreak the prospectively collected movements might vastly differ from the patient's movements during the height of infectiousness. Moreover, the GPS tracker can be unintentionally forgotten at home, and from a disease surveillance perspective, the increased level of privacy for the participants can also be a disadvantage as these missed locations can be of high epidemiologic interest.

Call Detail Records

Mapping individual movements in a population has become technically feasible by using call detail records (CDRs) systematically collected by telecom operators (6). CDRs consist of digitalized and organized information generated each time a mobile phone is used, e.g., calling, texting, connecting to mobile internet, and charging prepaid credit. CDRs include attributes such as a timestamp, source number, destination number, and most importantly for mobility mapping, the telephone mast (cell site) position showing the approximate geographic location. The spatial signal is less precise than what can be obtained by GPS tracking, as it results from assignment of the user to a telephone mast that is routing the call or text. The resolution is higher in urban areas (up to 50–100m in resolution) than in rural areas where fewer masts are placed.

A population-level analysis would benefit from the inclusion of all phone companies. While limited to active data points, no spatial information is available in the CDRs when the phone is not in use, the signal could be enhanced by sending short message service (SMS) messages to these targeted participants, generating an active data point for recording. An advantage is that mobile network operators typically maintain records for at least 3 months, allowing retrospective analysis of the period before transmission was interrupted by treatment, or the period before an outbreak is declared, and that this method is scalable to larger populations (7). Disadvantages include that persons of lower socio-economic status, children, and elderly persons might be underrepresented in the analyses, the lower spatial resolution in remote rural areas, and that details on phone sharing and double subscriber identity module (SIM) card use would need to be captured.

The use of CDRs provided by mobile network operators opens the possibility to map movements of large numbers of people (5,6,8), although expectations do not necessarily translate to impact (9). For instance, in Senegal mobile phone data of $\approx 150,000$ users were used to build

an epidemiologic model that highlighted the effect of mass gatherings on the spread of cholera in the country (10). A major hurdle associated with the potential utilization of CDRs for disease control purposes is that a third party, in this case for-profit mobile network operators, is involved in the research project. Conversely, from the mobile network operator perspective, this is data that they already collect, whether a study is happening or not. For them the ethical concern is that this data are shared with a third party, i.e. the researchers. This sharing of CDRs potentially increases the risks to the individual of confidentiality breaches. Mobile network operators in turn reflect on ethical aspects of public health or medical research use of CDRs (11).

References

1. Ruktanonchai NW, Ruktanonchai CW, Floyd JR, Tatem AJ. Using Google Location History data to quantify fine-scale human mobility. *Int J Health Geogr*. 2018;17:28. [PubMed](#)
<http://dx.doi.org/10.1186/s12942-018-0150-z>
2. Wesolowski A, Eagle N, Noor AM, Snow RW, Buckee CO. The impact of biases in mobile phone ownership on estimates of human mobility. *J R Soc Interface*. 2013;10:20120986. [PubMed](#)
<http://dx.doi.org/10.1098/rsif.2012.0986>
3. Wesolowski A, Stresman G, Eagle N, Stevenson J, Owaga C, Marube E, et al. Quantifying travel behavior for infectious disease research: a comparison of data from surveys and mobile phones. *Sci Rep*. 2014;4:5678. [PubMed](#) <http://dx.doi.org/10.1038/srep05678>
4. Jones KH, Daniels H, Heys S, Ford DV. Challenges and potential opportunities of mobile phone call detail records in health research: review. *JMIR Mhealth Uhealth*. 2018;6:e161. [PubMed](#)
<http://dx.doi.org/10.2196/mhealth.9974>
5. Wesolowski A, Buckee CO, Engø-Monsen K, Metcalf CJE. Connecting mobility to infectious diseases: The promise and limits of mobile phone data. *J Infect Dis*. 2016;214(suppl_4):S414–20. [PubMed](#)
<https://doi.org/10.1093/infdis/jiw273>
6. Erikson SL. Cell phones—self and other problems with big data detection and containment during epidemics. *Med Anthropol Q*. 2018;32:315–39. [PubMed](#) <http://dx.doi.org/10.1111/maq.12440>
7. Finger F, Genolet T, Mari L, de Magny GC, Manga NM, Rinaldo A, et al. Mobile phone data highlights the role of mass gatherings in the spreading of cholera outbreaks. *Proc Natl Acad Sci U S A*. 2016;113:6421–6. [PubMed](#) <http://dx.doi.org/10.1073/pnas.1522305113>

8. Sangokoya D, Letouzé E, Data-Pop Alliance. How to use big data? Leading experts' roadmap to data-driven innovation projects. Vodafone Institute for Society and Communications, editors. Berlin: Vodafone Institute; 2017 [cited 2019 Feb 7]. https://www.vodafone-institut.de/wp-content/uploads/2017/11/How-to-use-Big-Data_VFI_Data-Pop-Alliance-Paper.pdf
9. The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont Report: ethical principles and guidelines for the protection of human subjects of research. Pub. no. 78-0012. Bethesda (MD): The Commission; 1979.
10. European Union General Data Protection Regulation (GDPR). Frequently asked questions about GDPR [cited 2019 Feb 7]. <https://www.eugdpr.org/gdpr-faqs.html>
11. Council for International Organizations of Medical Sciences (CIOMS). International ethical guidelines for health-related research involving humans. 4th edition. Geneva: The Council; 2016.

Ethical Considerations for Movement Mapping to Identify Disease Transmission Hotspots

Appendix 2

Background, objective, participant's backgrounds, and agenda for the 1-day workshop on the ethical aspects on the use of individuals' mobility data for mapping infectious diseases held October 24, 2017, at the Institute of Tropical Medicine, Antwerp, Belgium

Workshop on the Ethics Surrounding Phone Tracking of Infectious Diseases

Background:

In the context of the development and review of the TB Enhanced Place Finding project, multiple ethical challenges were identified around the use of phone signals to see where tuberculosis (TB) patients crossed in time and space as a novel approach to identifying transmission hotspots.

Objective:

By inviting key experts and stakeholders, we aim to reflect on the risks and benefits of using tracking approaches by phone, global positioning system (GPS) signal, or otherwise for identification of transmission hotspots of TB and other infectious diseases, and on potential ways to reduce the risk. We plan to distil from this workshop an outline of a position paper that addresses challenges and solutions and ethical standards to consider when undertaking such efforts.

Participants:

- Ethicists, 2
- Scientists, 8, fields include epidemiology, bioinformatics, molecular biology, anthropology
- Information and communication technology experts, 2

- Data security specialists, 2
- Big data expert, 1
- Representatives of the Gambia Government and Medical Research Council joint ethics committee, 2
- Gambian National Leprosy and TB Programme representative, 1
- Expert on health, law, information technology, mobility data sharing, 1
- e-Health software provider, 1

Agenda

Part 1: Technicalities of phone tracking

- 9:10–9:30 The possibilities of phone tracking: TB phone tracking project in the Gambia, Enhanced Place Finding proof-of-concept project as introduction, to outline stakeholders and ethical challenges
- 9:30–9:50 Alternative approaches, such as global positioning system trackers: potential benefits and downsides
- 10:00–10:20 Phone tracking technology briefly described
- 10:30–10:50 The importance of informed consent and confidentiality agreements between all parties
- 11:10–11:30 Comprehension of the informed consent
- 11:40–12:00 The use of phone data from the perspective of an African regulator: How to protect consumer rights and government interests
- 12:10–12:30 The use of phone data from the legal and ethical perspective in Africa
- 12:30–13:00 Encryption, hashing and protection of privacy, Data Protection Impact Assessments (DPIAs) and General Data Protection Regulation (GDPR, EU Regulation 2016/679), a European perspective

Part 2: The future

- 14:00–14:30 Developing the app: technical and ethical challenges with implementation
- 14:30–14:45 Bigger picture, application for hotspot detection in other infectious diseases
- 14:45–15:30 Broader discussion
- Stigmatisation in infectious diseases

- Expand to other diseases: specific ethical challenges of phone tracking around
 - Sexually transmitted diseases/HIV
 - Malaria
 - Ebola....
- Using internet data rather than call detail records: technical and ethical challenges
- Could phone tracking be used in Europe, Asia, America, or other locations?

Part 3: Key aspects to be summarized in a position paper

15:50–16:50 Sum up and address the identified challenges, aiming for an outline of a position paper that addresses ethical challenges and solutions for phone tracking of infectious diseases.

Article DOI: <https://doi.org/10.3201/eid2507.181421>

Ethical Considerations for Movement Mapping to Identify Disease Transmission Hotspots

Appendix 3

Data Protection Impact Assessment template developed by White Wire Data Protection, Kontich, Belgium (following pages)



WHITE WIRE

Data Protection Impact Assessment

Document Implementation of DPIA For XXX

Performed by:	
Last update:	
Date of advice Data Protection Officer:	
Date Approved Directorate/Ethics Committee:	

1 Contents

1	Contents.....	2
2	Management Summary	4
3	Framework.....	5
3.1	Context Organization	5
3.2	Context processing /Project.....	5
3.3	Project Planning	5
4	DPIA Project Xxx.....	6
4.1	Scope.....	6
4.2	Relevant codes of conduct or certifications	6
4.3	(Joint) Controller	6
4.4	Concerned Actors	6
4.5	Categories of persons and personal data.....	6
4.5.1	Categories of data subjects.....	6
4.5.2	Categories of Personal data	6
4.6	Description of the processing in detail	6
4.6.1	Step 1: e.g. Providing information and gathering consent	6
4.6.2	Step 2	7
4.7	Processors and processor agreements	7
4.8	Compliance with basic principles for processing of personal data	7
4.8.1	Lawfulness, Fairness, and Transparency (information)	7
4.8.2	Purpose	7
4.8.3	Minimal data processing.....	7
4.8.4	Accuracy.....	7
4.8.5	Storage limitation.....	7
4.8.6	Integrity & Confidentiality.....	7
4.9	Rights of the data subject	8
4.9.1	Possibilities for exercising rights of the data subject.....	8
4.9.2	Right to Information.....	8
4.9.3	Right of Access	8
4.9.4	Right to Rectification.....	8
4.9.5	Right to Data Erasure	8
4.9.6	Right to limitation of processing.....	8
4.9.7	Right to portability	8
4.9.8	Right of objection.....	8
5	Risks.....	9
5.1	Risk methodology	9
5.2	Identified risks	9
6	Measures taken	10
6.1	RISK-001: Legal Position of Controller	10
6.2	RISK-004: Use National Identification number without permission	10
6.3	RISK-005: U.S. hosting provider	10



7	Residual risks.....	10
7.1	Overview residual risks.....	10
7.2	Advice from the DPO.....	11
7.3	Decision on prior consultation with DPA.....	11

2 Management Summary

This document documents a Data Protection Impact Assessment (DPIA) as described in the General Data Protection Regulation. This DPIA is an analysis of the intended processing of personal data for Project XX and contains the general context, information on the processing, assessment of the inherent and residual risks and concrete measures to be taken to mitigate these risks, and includes a formal advise on the need for prior consultation with a Data Protection Authority (DPA).

Further summary of the DPIA.

3 Framework

3.1 Context Organization

Describe the organization, its tasks and other information relevant in the context of the DPIA. This information serves to clarify why this organization intends to carry out the proposed processing.

3.2 Context processing /Project

General description of the project, for full details see 4.5.

Continuing on 3.1, how does this process connect to the context of the Organization.

3.3 Project Planning

If the DPIA is part of an ongoing project, describe the general planning and deadlines, including the time table of execution of the DPIA. This is especially useful in projects with a tight schedule where the performance of a DPIA should be carefully orchestrated.

4 DPIA Project Xxx

4.1 Scope

What is included and what is excluded in this DPIA. This can relate to specific aspects of research or to clarify which tools or processing have or have not been taken into account.

4.2 Relevant codes of conduct or certifications

Are there any codes of conduct or certifications relating to data protection applicable to the intended processing, or the sector of the controller?

Does the controller meet these codes of conduct/certifications?

4.3 (Joint) Controller

Who is the controller? Sometimes this is simply the organization itself, in other cases there may be partnerships where the determination of the respective responsibilities is an essential part of the DPIA to correctly document joint controllerships and the responsibilities it entails.

4.4 Concerned Actors

List of relevant organisations and persons incl. their function. Think of stakeholders such as the relevant data protection authorities, individuals (clients, patients, residents, etc), interest groups, the Data Protection Officer (DPO), processors, etc.

4.5 Categories of persons and personal data

4.5.1 Categories of data subjects

Whose personal data are processed within the scope of this DPIA? (Employees, patients, clients, residents, research participants, users, etc.)

4.5.2 Categories of Personal data

Which categories of personal data are processed? Include non-sensitive personal data (identification data, financial data, etc) as well as sensitive personal data (articles 9 and 10 GDPR)

4.6 Description of the processing in detail

By means of diagrams or simply text, present the data flow, from reception or creation of the data to eventual destruction, archiving or forwarding, also called the data life cycle.

This section should also establish whether there will be any forwarding of data to third countries and whether these third countries offer adequate protection (possibly by reference to other relevant parts in the DPIA).

4.6.1 Step 1: e.g. Providing information and gathering consent

4.6.2 Step 2

4.7 Processors and processor agreements

Which processors are involved in the processing, and are appropriate agreements in place (processor agreements or DPA's (data processing agreements)) as described in article 28 of the GDPR?

4.8 Compliance with basic principles for processing of personal data

Given the information in 4.1 and 4.3, please specify compliance with the basic principles of processing.

4.8.1 Lawfulness, Fairness, and Transparency (information)

Describe the manner in which information is provided to the data subject and the legal basis for the processing of personal data with special attention to "legitimate interest".

If relevant, also describe in which way there has been communication with stakeholders or representatives, interest groups, and the request for their opinion.

4.8.2 Purpose

What are the clear, specifically defined purposes of data processing?

4.8.3 Minimal data processing

Given the Purpose mentioned in 4.8.2, which personal data is required? (Categories of data or effective listing of all data) Are only those data processed?

4.8.4 Accuracy

Is the data that is processed accurate and correct? (links to other data sources to keep data up to date, periodic pop ups for the user to review data, online portal for stakeholders, etc.)

4.8.5 Storage limitation

What is the retention period of the data, and why exactly that retention period? Sometimes this is laid down by law, sometimes it has to be substantiated by a specific justification.

4.8.6 Integrity & Confidentiality

How are confidentiality, integrity (and availability) of the data secured?

To test these criteria, the domains from the ISO27002 are used as the basis. Other standards or certificates obtained may also suffice as a justification for providing the appropriate measures to ensure the integrity, confidentiality and availability of data.

- 4.8.6.1 *Security policies*
- 4.8.6.2 *Risk Analysis and remediation plans*
- 4.8.6.3 *Appointment of a DPO*
- 4.8.6.4 *Organization of Information security*
- 4.8.6.5 *Human Resource Security*
- 4.8.6.6 *Asset Management*
- 4.8.6.7 *Access Control (logical)*
- 4.8.6.8 *Cryptography*
- 4.8.6.9 *Physical security*
- 4.8.6.10 *Operational security*
- 4.8.6.11 *Communication security*
- 4.8.6.12 *System acquisition, development and maintenance*
- 4.8.6.13 *Supplier and processing relations*
- 4.8.6.14 *Security incident management*
- 4.8.6.15 *Business Continuity Management*
- 4.8.6.16 *Compliance & Accountability*

4.9 Rights of the data subject

In the first instance, it is necessary to describe how a data subject can exercise his/her rights, i.e. via a telephone number that can be called, physical location to visit, email address to write to, etc., or any other way a data subject can exercise his or her rights (section 4.9.1).

The following sections address the different rights: are they applicable, when, and how is compliance assured (e.g. online portal, request by email according to process described in 4.9.1).

- 4.9.1 *Possibilities for exercising rights of the data subject*
- 4.9.2 *Right to Information*
- 4.9.3 *Right of Access*
- 4.9.4 *Right to Rectification*
- 4.9.5 *Right to Data Erasure*
- 4.9.6 *Right to limitation of processing*
- 4.9.7 *Right to portability*
- 4.9.8 *Right of objection*

5 Risks

Listing of detected risks without additional measures taken (inherent risk). In other words, we are now reviewing the situation based on the description in the previous chapters. What are the risks or problems we identify in relation to the data we process (e.g. the basic principles of personal data processing, security of the information), and in a broader context, the possible impact on persons whose data are processed (e.g. Rights of the individual, reasonable expectations, sensitivity of the data, possible consequences of a data leak).

In Short: once all previous chapters have been completed, there are most likely deviations or aspects that require further scrutiny. Examples are included below including an estimation of severity.

5.1 Risk methodology

How are the risks estimated or identified (through interviews, analysis of documentation, risk assessment criteria etc) and based on what criteria is a severity assigned to the risks? This requires a description of how risk is measured. Ideally these scores or measurements are objective: if person X performs a risk analysis and person Y performs the same analysis later, the same scores will be applied due to the objective nature of the scoring criteria.

5.2 Identified risks

Nr	Description	Severity	Chapter
RISK-001	Ambiguity: Joint processing officers or one processing officer, namely the Xxxx?	Low	4.2
RISK-002	Enter Xxxxx File number to copy data: How unique are these file numbers? Other ' acquisition of other file functionalities '?	Low	4.2
RISK-003	Data subjects are not adequately informed due to language barriers	Middle	4.3
RISK-004	Intended use of the National Identification number without the authorisation of the SC	Critical	4.6
RISK-005	Xxxxx uses U.S. hosting, and may also process the National Identification number	High	4.7
RISK-006	Retention periods have not yet been validated	Middle	4.8.5
RISK-007	Logging currently provided is not sufficient to track all create, read, update and delete (CRUD) actions on personal data (test to be validated)	Middle	4.8.6
RISK-008	Xxxx Does not possess a compliant Processing Agreement	High	4.8.6
RISK-009	Web application that is accessible to the public and will possibly process National Identification number : no penetration testing provided.	High	4.8.6
RISK-010	Default setting includes Transfer to XXX, does not adhere to data protection by default principles	High	4.8.1

6 Measures taken

Describe what measures have been taken to mitigate the risks as identified in 5.2. This usually involves reference to a risk number and a description of risk treatment (how has a risk been addressed). Risk treatment can involve for possible treatments (in order or preferred approach):

- Avoidance: ensure the risk cannot take place by completely eliminating it
- Transfer: the risk still exists, but is now the responsibility of someone else
- Mitigation: some residual risk may exist, but measures have been taken to mitigate the risk as much as possible
- Acceptance: no treatment except the realization that the risk can occur and no specific measures will be taken to reduce it (further).

6.1 RISK-001: Legal Position of Controller

6.2 RISK-004: Use National Identification number without permission

6.3 RISK-005: U.S. hosting provider

7 Residual risks

Analyse here which of the risks identified in Chapter 5 are not adequately covered by measures in Chapter 6. These are the residual risks. Below you will find an overview of various potential risks that cannot be covered by the various measures (i.e. residual risk).

7.1 Overview residual risks

No	Description	Ernst	Chapter
RISK-001	Lack of a privacy policy	Critical	4.1
RISK-002	Absence of an information security plan	Middle	4.2
RISK-003	Access control (logical) of application X is insufficient	High	4.3
RISK-004	Access control (logical) to file server has no assigned roles	Middle	4.6
RISK-005	No clearly defined or determined purpose	Critical	4.5
RISK-006	Processing agreements are not in place	Critical	4.7

7.2 Advice from the DPO

If appointed, it is mandatory to involve the DPO in the execution of the DPIA¹. Concerning the analysis in this document, what advice does the DPO have regarding the processing (s) that forms part of the DPIA? Proceed with the processing? Specific residual risks that still need to be addressed? Is prior consultation with the Data Protection Authority warranted?

7.3 Decision on prior consultation with DPA

Depending on the residual risks from 7.1, it is stated here whether a prior consultation with the Data Protection Authority is required. In other words, whether the local data protection authority should be contacted to ask for advice on processing because the residual risks are (possibly) too high.

If relevant, include the approval or reference to a report from a project team, management consultation, etc. where the decision on the prior consultation has been discussed.

-----End of Document-----

¹ Art 35.2 GDPR