NIST Special Publication 1268

Workshop Report: Challenges for Digital Proximity Detection in Pandemics: Privacy, Accuracy, and Impact

Michelle Stephens
Greg Cala
Kristen Greene
Kathryn E. Keenan
Angela Robinson
Lu Shi
Don Ufford
Zachary Valdez

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1268

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 1268

Workshop Report: Challenges for Digital Proximity Detection in Pandemics: Privacy, Accuracy, and Impact

Michelle Stephens
Greg Cala
Kristen Greene
Kathryn E. Keenan
Angela Robinson
Lu Shi
Don Ufford
Zachary Valdez
National Institute of Standards and Technology

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1268

May 2021

U.S. Department of Commerce
Gina Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Special Publication 1268
Natl. Inst. Stand. Technol. Spec. Publ. 1268, 32 pages (May 2021)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1268

Preface

The recommendations contained herein are those of the authors, derived from discussions held during the workshop, and should not be construed as official policy of the Department of Commerce (DOC). This document does not convey official policy of DOC or the National Institute of Standards and Technology (NIST), nor does it suggest who should be responsible for taking actions identified in the recommendations.

Abstract

NIST held a three-day workshop, "Challenges for Digital Proximity Detection in Pandemics: Privacy, Accuracy, and Impact" Jan. 26th – 28th, 2021. Members of industry, academia, non-profits, state, and federal government were brought together to discuss successes and challenges associated with implementation of proximity detection technologies and to identify areas in which additional effort is required. The first day featured invited speakers on a variety of aspects of proximity detection and the existing challenges. The second day featured a panel discussion and facilitated break-out sessions to provide opportunity for community engagement on ways to overcome the challenges presented in the first day. The final day included reports from the break-out sessions, contributed technical talks, and a wrap-up discussion. This document provides an overview of the presentations and discussions and describes key themes that emerged during the workshop. The agenda, video of the invited talks on Jan. 26th and of the panel discussion on Jan. 27th, and slides from the contributed talks are available on the website, https://www.nist.gov/news-events/events/2021/01/challenges-digital-proximity-detection-pandemics-privacy-accuracy-and .[1]

Key words

Exposure notification; Google/Apple Exposure Notification (GAEN); proximity detection

Acknowledgements

We are particularly indebted to Marc Zissman from MIT Lincoln Laboratory and his colleagues with the MIT PACT organization for their suggestions on topics and help identifying and recruiting speakers and panelists. Thank you also to our breakout session facilitators, Ashley Boggs, Callie Higgins, Leah Kauffman, Jeremy Lawson, Jeanita Pritchett, Jessica Staymates, and Brandi Tolliver, and to the scribes, Greg Cala, Angela Robinson, Don Ufford, Zach Valdez, Katy Keenan, Lu Shi, and Kristen Greene.

Workshop funding was provided by the NIST Computer Security Division, Information Technology Laboratory, and Applied Physics Division, Physical Measurement Laboratory.

NIST Organizing Committee

Heather Evans	Naomi Lefkovitz	Rene Peralta	Krister Shalm
Katy Keenan	Nader Moayeri	William Ratcliff	Michelle Stephens
Mark Keller	SaeWoo Nam	Angela Robinson	

[1] The workshop videos and this publication include external perspectives from industry, academia, government, and others. The opinions, recommendations, findings, and conclusions do not necessarily reflect the views or policies of NIST or the United States Government.

Table of Contents

1. Executive Summary

Digital proximity detection (DPD), or "automated exposure notification," emerged in 2020 as a tool for combating the COVID-19 pandemic. As the field has developed, it has become apparent that this tool has the potential to provide information to the public, to public health officials, to building designers, and many others. This information could be used to help prevent future outbreaks. It is a uniquely multi-disciplinary field that requires the integration of diverse areas of expertise such as privacy, public health, sociology, economics, law, ethics, ranging technologies, human design, and epidemiological modeling, to name a few. Until recently, many of the experts in these areas didn't work together on a professional basis and so are working now to build an understanding of each other's fields. NIST's research efforts in cybersecurity, privacy, metrology, public safety, and resilience incorporate much of the expertise within a single organization, and for that reason NIST held this workshop to give members of the community an opportunity to engage with each other, and to support this new community and its important work.

A total of 98 attendees from around the world participated in this virtual workshop. Roughly 1/3rd of the attendees was from U.S. federal organizations, 1/3rd from academia, and the remaining third represented other groups including industry as well as nonprofit and not-for-profit organizations. NIST used a Slack workspace for all attendees during the workshop as a collaboration platform for more detailed discussions and one-on-one conversations between participants. Many registrants joined the Slack workspace, and 58 actively posted in the workspace.

Several key themes emerged over the course of the workshop, including:

- Automated exposure notification (AEN) is a tool that augments manual contact tracing but does not replace it.
    - Manual contact tracing includes aspects of support, health advice, cultural understanding, and a legal basis for quarantine that AEN does not achieve.
    - AEN can reach people not personally known to an index case, still works when manual contact tracing exceeds resource limits, can be set up to privately and automatically notify someone of a possible infection, can offer notified users choices of how to respond, allows each public health authority to set an operating point based on its risk-benefit analysis, and it may be faster to notify possible infections than manual contact tracing.
- Early data show that the Google Apple Exposure Notification (GAEN) does have an impact and does identify contagious contacts; however, whether it is "effective" is still under discussion, as even the definition of "effective" is different for different stakeholders. The contributions are relevant, and the systems are not overly expensive.
- The field needs much more data to evaluate the performance at all levels, from device performance to public health efficacy. There is a trade-off between gathering some of this data and maintaining individual privacy.
- There are significant challenges to public acceptance of AEN. These include privacy concerns, finding a value proposition to increase participation by individual users, and messaging that is consistent and understandable.

- Intermingling public health efforts with those of a few private, for-profit companies in the way that GAEN does is a new paradigm and one that raises concerns of some stakeholders over privacy, transparency, long-term motives (for example, public good vs profit), and potential stifling of innovation.
- This is a broadly multidisciplinary endeavor; it is important to include all stakeholders at all phases in development, implementation, and evaluation of effectiveness.
- AEN technology should be designed to detect disease transmission, not just proximity. Technological metrics such as Bluetooth accuracy should be related back to actual performance in terms of disease spread and population health outcomes.
- There are many opportunities for future technical innovation and broader applications. These include improving transmission detection with the use of stationary beacons and/or augmented sensors (for example to detect whether the user is indoor or outdoor), adapting the technology to provide encounter metrics that can inform improved building ventilation design and occupancy limits, or to gather other epidemiological data.
- Issues of equity and efficacy for different user populations need to be addressed, especially if solutions are tied to ownership of smartphones.
- Wearables (e.g., bracelet or lanyard devices) that are not dependent on smartphones could address some of the potential issues voiced by stakeholders around privacy and access.

Some of the actions for the future suggested by participants include:

- Continue the multidisciplinary dialogue within this diverse AEN community to match needs with technical developments. Engineers can implement a variety of technologies but must interface with key stakeholders to ensure they are solving the most important problems.
- Do not view GAEN as a final solution. It was developed quickly out of necessity, but the design should be revisited in the future.
- There needs to be a coherent communication strategy to the public. Messaging needs to be consistent and more understandable. The AEN community needs to show both that AEN works and provides value to individual users.
- We need more data to quantify performance and impact, both at the public health level and for the underlying proximity detection technologies e.g., multi-sensor technologies could be developed to enhance verification.
- Multi-sensor technologies combined with machine learning (ML) could be very powerful. For example, sensors could be used to determine airflow characteristics, and artificial intelligence (AI) and ML could be used to indicate potentially infectious building issues, or they could be used to implement outdoor-vs-indoor contact identification to account for differences in infectiousness for COVID-19 in different environments.
- Develop a data toolbox that can be used to evaluate technologies for future pandemic analyses.
- Evaluate the use of wearables (e.g., non-smartphone approaches) to address considerations like privacy and implementing solutions for smaller communities such as workplaces or living facilities.

- Investigate broader applications such as building design, encounter metrics, and epidemiological monitoring.
- Investigate stationary beacons to improve effectiveness and target super spreader events (estimated to be responsible for 80% of COVID-19 infections[2]) as well as enable broader applications such as encounter metrics for building design.
- Government involvement is needed in privacy guidelines and standards development. There is a need and desire for documentary standards in areas of privacy protocols specific to exposure notification, performance of ranging technologies, and other aspects of AENs.
- Government should continue to convene resources, stakeholders, etc. to facilitate these sorts of discussions.
- Federal-level guidance would be helpful to understand potential implications of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) law and to reduce misinterpretations of law and policy for these applications.
- Developers of AEN must consider the ownership of the infrastructure for the future. If it's under the control of for-profit organizations, what implications are there for future developments?
- Looking to the future, how can AEN be platform/technology-agnostic? What will we carry ubiquitously in the future? Wearable/embedded technologies? Consider threats such as bioterrorism and how we might address future customized virus creation.

Anonymous participant: "Digital proximity detection in its current form is overshadowed by Google Apple Exposure Notification and the current pandemic, but there seems to be a very interesting ecosystem developing related to digital health (interaction of personal electronics and healthcare)."

1. Introduction

The workshop "Challenges for Digital Proximity Detection in Pandemics: Privacy, Accuracy, and Impact" was held virtually Jan. 26, 2021 – Jan. 28, 2021. Members of industry, academia, nonprofits, not-for-profits, and U.S. state and federal government were brought together to discuss successes and challenges associated with implementation of proximity detection technologies and identify areas in which additional effort is required. The first goal of the workshop was to provide the community, which comes from a diverse set of backgrounds, with a holistic understanding of the concept and challenges behind automated exposure notification (AEN) from all perspectives. To that end, the first day was a series of invited talks that tried to cover as many different aspects as possible. Second, we wanted to provide the community with an opportunity to discuss these multi-faceted challenges, potential solutions , and what actions should be taken. On the second day we held a panel discussion followed by smaller break-out sessions with facilitated discussions on targeted topics chosen by the workshop participants. The final goal of the workshop was to work together to identify and document priorities and challenges for both the short- and long-term future. To that end, on the third day, we reconvened for a series of more technical talks and a

[2] Endo, A. *et al. Wellcome Open Res.* 5, 67 (2020).

workshop-wide discussion. NIST hosted a Slack workspace throughout the workshop to provide a collaborative platform for more detailed discussions and one-on-one conversations between participants.

2. Invited Speakers

This section provides a summary of the invited talks presented on the first day. The talks were videotaped and are available for viewing at https://www.nist.gov/news-events/events/2021/01/challenges-digital-proximity-detection-pandemics-privacy-accuracy-and.

The first two invited speakers, Joanna Masel and Marc Zissman, gave high-level overviews of exposure notification opportunities and challenges. Dr. Masel discussed the challenges of interdisciplinary problem solving and provided some advice on how to find the right expert to talk to, along with a warning to beware of misconceptions propagated by non-experts. She discussed the existing "Too Close for Too Long (TC4TL)" design specification of less than 6 feet of distance for more than 15 minutes that at the time of the workshop was used for both manual contact tracing and AEN, based on U.S. public health guidance. She discussed the limitations of this specification and how AEN can be developed to use improved metrics for risk of infection. She has developed a mathematical framework for evaluating risk and pointed out that human behavior is as important a factor as the physics of the interaction. Moving forward she suggested enhancing GAEN by targeting super spreader events with broadcast-only beacons (discussed in more detail by James Petrie in a contributed talk).

Dr. Zissman presented a brief tutorial of the Google Apple Exposure Notification (GAEN) approach. GAEN is compatible across U.S. state boundaries and in use in 30 countries in Europe and North America. He described the different layers of GAEN: Layer 1 Proximity Measurement, Layer 2 Private Cryptographic Protocol, Layer 3A Public Health Interface (for example, verification codes, etc.), and Layer 3B Individual Interface (for example the specific app used). He showed assessments of effectiveness with a specific example of early data from Switzerland showing AEN is faster and finds infected people manual contact tracing would miss. Dr. Zissman also discussed the TC4TL definition and how standard parameter sets were defined in an international workshop and differ in thresholds to provide more or less risk balanced with probability of false alarms. He pointed out that more analysis is needed to understand operating points, then developers can let public health choose where they want to operate. Dr. Zissman stressed that as engineers they can implement anything but rely on others to define needs and requirements for them.

The next two invited talks addressed the effectiveness of AEN and what is needed to make a difference in epidemiological terms of combating the COVID-19 pandemic. Dr. Luca Ferretti presented modeling results that show it is difficult to achieve the required parameter space over which contact tracing is effective using the technologies employed currently. These models show contact tracing is only effective when it has high efficiency and short response times. This provides an argument for augmenting manual contact tracing with AEN. Effective AEN relies on integration with local health policy, high user uptake and adherence, quarantining as accurately as possible, rapid notification, and an ability to evaluate effectiveness transparently. However, Bluetooth apps require individuals to download them, open them and set them up, enable Bluetooth, share contacts, and share codes for positive

tests, which negatively impact user uptake and adherence. Privacy considerations limit access to information needed to evaluate effectiveness. Dr. Ferretti's modeling predicts that 60% uptake is required to make AEN a stand-alone solution (i.e., to create "digital herd immunity") within the public. No country has achieved that level with voluntary uptake. However, he went on to show that the critical limit for adoption of AEN to make any impact is around 15%. Furthermore, uptake is typically clustered, so that while total uptake may be low, high local uptake can lead to community risk reduction. He discussed this from two perspectives: epidemiological effectiveness and personal protection. His modeling shows that despite low uptake there can still be a 4X impact at the population level (epidemiological effectiveness), and a 14X impact at the personal level (personal protection), because people who use the app tend to be clustered. Early results from real life validation based on usage information from Spain show a 2X impact.

Dr. Viktor von Wyl continued the discussion of real-life validation by describing his studies of the SwissCovid app experience. He began by making the point that privacy considerations make it difficult to study effectiveness and stressed the importance of leveraging existing research studies and data. Results from a study embedded in Contact Tracing of the Canton of Zurich show that SwissCovid-notified contacts with exposure risk outside their own household entered quarantine 1 day earlier than manually notified contacts. This is significant for reducing the spread of Covid-19. Another study also focused on the Canton of Zurich. In that effort 30 people tested positive for coronavirus after receiving an app notification.

These results show that GAEN apps can be relevant in the public at modest adoption levels. Implementation of these apps is relatively low-cost. Dr. von Wyl also discussed how the upstream and downstream systems that interact with the AEN system really matter. He discussed procedural bottlenecks early on that were later resolved such as delivery delays for COVID codes (an individual with the app would test positive but there was a delay in receiving the code to upload so that his or her contacts could be notified), unmet communication needs (by users, other actors), and fears for resource competition (time and money) from already overtasked manual contact tracers. Another barrier is that because the SwissCovid app is so privacy preserving, it is hard to evaluate effectiveness, and people felt it wasn't doing anything so therefore didn't use it. A recent survey showed that 46% of the population have downloaded the app. The top three reasons for non-use are (1) not the right phone; (2) privacy concerns; and (3) not perceived as useful.

The next two speakers discussed public acceptance and public health concerns. The first, ethicist R. Alta Charo, drew on lessons learned in her work on emerging biotechnologies. She noted that initial excitement around public health advances is often quickly turned into cautionary tales and emphasized the need to build features into the design of new technologies to address potential concerns. These aspects of the design could be engineering, legal, or other. Coupled with this one needs a communication strategy; she pointed out that it's often helpful to discuss technologies in terms of personal advantages to health rather than public health. For AEN specifically, Charo noted it's important to reassure the public about how the technology addresses issues that they may care about, for example not causing unnecessary quarantines and the privacy of their data. A real-world example that is in the

public's mind is how genetics databases originally hosted by private companies to help trace ancestry later became monetized and ultimately also used by police. Experiences like this can lead to a distrust of new technologies, for example, concerns that data will ultimately be used in ways beyond those originally promised. Without a deep understanding of the engineering behind AEN, the general public may also believe they are being tracked and further distrust the technology although there is already much loss of anonymity in the form of toll booth cameras, CCTV cameras, doorbell cameras, RFID readers in buildings, and, of course, the internet. We know that people will relinquish this information either because they think they are getting something back or because they don't understand; often the allure of a benefit can overcome serious privacy concerns. Charo pointed out that built-in user controls and information about where and how long data are kept can help mitigate these potential concerns.

Meghna Patel provided a public health perspective by discussing the Pennsylvania Department of Public Health's experience to date with the COVID Alert app. In the interest of expediency, the state chose to work with a company that had already developed exposure notification apps that used GAEN. The state felt that Apple and Google had made clear the need for strict privacy protocols. Because of the many limitations of AEN (e.g., inaccuracies of Bluetooth around metal, inability to know if masks were worn, measuring phone-to-phone distance and not person-to-person distance, and public mistrust of technology in the time of a misinformation pandemic). The state implemented the app with a goal of identifying unknown and unfamiliar person interactions to augment their manual contact tracing. To combat misinformation about data security, the state required that the app be open-sourced. The app uses the Association of Public Health Laboratory (APHL) server and is interoperable with many states. At the time of the workshop, 7.6% of the eligible population in PA had downloaded the app. By embedding questions about the app with those asked by manual contact tracers, the state has determined that 3% of positive cases on average have the app installed. Of the 3%, nearly half (about 47%) actually upload the random ID they are given that will notify their contacts. One set of data shows this led to 529 exposure alerts and 70 requested call-backs from the Department of Public Health. A highlight of that study is that one callback received an exposure alert and tested positive, resulting in identifying a possible asymptomatic case. Lessons learned so far are that this technology cannot replace manual contact tracing, but it can accelerate distribution of alerts to the unknown and unfamiliar contacts. Patel emphasized the need for public health authorities to message what information they do and do not collect. To be clearly understood, this message should be framed as a public health communication and phrased in 6th grade language. One barrier to effectiveness of the app that Patel shared is that many people who test positive are not willing to upload the code to notify their contacts. Rather, they downloaded the app to protect themselves. Some who work in a small work environment don't want to be seen as the person who made others sick or must quarantine. Pandemic fatigue along with other overlapping crises, differences in messaging at different levels, and low uptake of technology doesn't help. Patel noted that further research of interest includes how AEN can work with other infectious diseases, ways to increase trust in public health and privacy, and how to highlight messaging techniques to increase adoption.

The third part of the invited talks took a deep dive into privacy and security, featuring three perspectives. First, Naomi Lefkovitz gave an overview of privacy considerations from NIST's perspective. NIST approaches privacy as a risk-management process, rather than thinking of privacy as a binary condition. Privacy gains or losses are considered as a continuum and residual risk is evaluated. This helps users and implementers make informed decisions and provides a start to understanding what the privacy gains and losses really are. She provided two examples of how the NIST privacy framework was used to assess AEN privacy risks. In the first example, she showed how policy considerations can be applied to different types of AEN solutions, not just GAEN. Different implementations may lead to different policy considerations (for example opt-in or opt-out, how is data stored and disposed of, are other uses of data permitted). The choices made may be different depending on whether it is a workplace or a public health authority making the decisions. The second example focused on technical capabilities, for example different outcomes for associating a device with a person, centralized vs decentralized data. Some new research shows counterintuitive perceptions between risks of centralized and decentralized systems. The privacy framework helps organizations to consider what privacy capabilities they want for their solution and understand tradeoffs. It allows organizations to generally evaluate the operating environment. Some choices might only be possible in a limited community. For example, some companies already provide wearables. These can also be used for social distancing and AEN, but they weren't necessarily designed for that, so implementers need to think about privacy considerations. Function creep is an important issue for privacy professionals.

Second, Rene Peralta specifically discussed privacy preserving protocols for encounter metrics and how to be prepared for the next pandemic by considering use of these technologies to engineer environments to slow the spread of disease. He introduced the idea of encounter metrics in which the technology detects an encounter, labels the encounter (but not the parties), evaluates the length or severity, and aggregates and derives encounter metrics statistics. The encounter metrics can be used for contact tracing or to engineer our working environments. This is unlike some of the existing protocols including GAEN that expose the pseudonyms of the infected people and therefore may also be exposing the identities. He referred to the four principles outlined in an open letter on contact tracing signed by over 300 scientists[3] and discussed that it is problematic if these technologies are subordinate to commercial processes and constraints, if the system is built on top of a surveillance platform like a smartphone, or if the public is not given low level access to the platform, as with GAEN. Independent wearables can be designed to address these principles.

The third speaker, Seda Gürses, discussed privacy by design as an infrastructural power. Rather than talk about merits and weaknesses of GAEN, Seda Gürses discussed her views of how privacy (perhaps counterintuitively) became a way for larger private companies to center their services and expand their power, at detriment to the agency of users and governments as well as researchers. AEN has provided tech companies an opportunity to gear up their cloud infrastructure in a way that offers them growth into the public health

[3] Joint Statement on Contact Tracing: Date 19th April 2020, https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view .

sector. While developing the Decentralized Privacy-Preserving Proximity Tracing (DP3T)[4] protocol it was assumed that governments would have a say in design, deployment, etc. However, as soon as the government said 'we want apps' it was necessary for the developers to cooperate with large tech companies. For example, so as not to drain the battery, app developers needed low-level access to smartphone Bluetooth API. Phase 1 of the development provided access to the interface but also allowed privacy to become a way for large tech companies to exercise infrastructural power through design. Phase 2 was implementing GAEN into smartphone operating systems. This reconfigured all actors involved. Apple and Google could push functionality onto all phones under their control, although users still must turn on the app. Use of the technology is no longer limited to countries or states, which can be a benefit; however, in the US, it also meant that the tech companies were introduced as an arbiter between states. Phase 2 also reduced the possibility of transparency and limited possibility to do research on data, although, admittedly, the data have limited value. Gürses asked the audience to consider that Google and Apple are now gatekeepers, requiring the government to collaborate with them. While it was faster, more scalable, and less costly to use existing computational infrastructure than anything governments could build, this does pave the way to producing public health as a computational infrastructure owned by private companies. She asked the audience to consider several questions, including: What does it mean to do public health using a computational infrastructure that is run by companies who by virtue of owning their infrastructure can determine the design of apps and conditions of use? What kind of public health are we imagining by doing so? What does it mean to lean our science on a computational infrastructure which would tightly knit our public health to big tech and their financial circumstances? What would it mean as scientists to always have to go to tech companies for data and to do science? Can we call population management through behavioral engineering and optimization from a central vantage point democratic? How do we deal with the risk that some of the well-intended optimization of behavioral change we study becomes part of an infrastructure that is not just subject to public interest but also the bottom line of large tech companies? Gürses concluded her talk by emphasizing that designing for privacy should limit accumulation of data, but using these metrics, privacy is power. Current AEN solutions do limit surveillance, but they allow computational infrastructures for optimization of population management, potentially at the expense of democratic institutions.

The day of talks concluded with two talks highlighting some of the challenges and potential solutions to overcoming technological limitations of AEN. Dr. Po-Shen Loh discussed his thoughts on reducing the spread of COVID by flipping the perspective: developing solutions for which everyone has incentives to participate and behave in ways that minimize disease transmission. He described how the NOVID app arose from this perspective. Rather than relying on the traditional contact tracing paradigm that identifies sick people and separates them from everyone else by quarantining them, Dr. Loh suggests using a radar paradigm that can let healthy people anonymously see the disease coming, so they can avoid it. This paradigm reduces the user's chance of both infection and quarantine; from Loh's perspective installing a standard contact tracing app increases the user's chance of quarantine, while only

[4] see for example, C. Troncoso et al., *Decentralized privacy-preserving proximity tracing*, Apr 2020, [online] Available: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.

reducing everyone else's chance of infection (not the user's). The NOVID app flips the incentive for downloading and using an app to give users the power to make informed decisions to protect themselves, rather than receive unenforceable requests to quarantine to protect others. It doesn't ask users do anything inconvenient such as quarantine. Adoption in pilots at Georgia Tech and Carnegie Mellon University have shown that when a few people download the app more follow, and survey results show that people do indeed make changes to their behavior when they see COVID cases rising a few degrees of connection away from them. For example, they choose to social distance more. Other problems with existing AEN systems that the flipped perspective addresses include reducing the number of "unnecessary" quarantines and resulting 'quarantine fatigue.' Dr. Loh cited reports that the probability of an unmasked 15-minute interaction at six-foot distance leading to an infection is under 10%. Given that, Dr. Loh posited, a typical AEN system that notifies an individual to quarantine based on such an interaction may be directing people to quarantine "unnecessarily" 90% of the time, often at great inconvenience and no benefit to the individual. By flipping the perspective to allow people to be informed of how 'close' they are to an infection, the NOVID app incentivizes people to change their behavior to avoid infection, not necessarily to quarantine after possible infection, for self-protection. Another problem is that many asymptomatic and untested positive cases are not captured. Using the law of large numbers, radar still detects a cloud of cases approaching to boost caution.

Omid Sadjadi concluded the day with a discussion of the NIST Too Close for Too Long (TC4TL) challenge. He described the challenge and gave an overview of the results. NIST held the machine learning challenge in collaboration with MIT PACT to help advance Bluetooth-based proximity detection technology through evaluation-driven research. It provided a common testbed to explore promising ideas in proximity detection using Bluetooth Low Energy (BLE), support the research community, measure impact of additional sensor information such as accelerometers, gyroscopes, etc., and measure the performance of state-of-the-art. The challenge task was proximity detection. This is challenging because BLE is a very noisy indicator. There are large variations in signal strength depending on the immediate environment, there can be multi-path signals, the signal varies with orientation of the devices relative to each other and whether they are held in hands, in pockets, or in purses (i.e., phone carriage states). The smartphone model and the user's posture also influence the signal. The challenge primarily used datasets provided by the PACT and MITRE organizations. Eleven teams participated in TC4TL from both academia and industry. To summarize the results: machine learning seems to be viable and able to provide some benefits across the board. There is great variety in the phone carriage states, showing that it is important to evaluate multiple states. The GAEN API only provides a limited amount of data, to unleash full potential of machine learning systems requires a lot more data. Final observations are i) ML-based proximity detection seems viable, but generalization remains an issue, ii) the hand-held condition is the best performing (this is the condition that is most akin to free space), iii) more looks into BLE sequence appear to improve performance, and iv) the availability of carriage-state metadata does not impact performance, but post-challenge efforts found benefits to the availability of such metadata.

3. Panel Discussion: The effectiveness of digital proximity detection at limiting the spread of infectious diseases

- Dr. Krister Shalm (moderator) Applied Physics Division, NIST and Physics Department, University of Colorado, Boulder
- Dr. Marc Zissman, Associate Head, Cyber Security and Information Sciences Division, Lincoln Laboratory, Massachusetts Institute of Technology
- Dr. Po-Shen Loh, Founder of NOVID, Professor of Mathematical Sciences at Carnegie Mellon University, and National Coach of USA International Math Olympiad team
- Mr. Mike Judd, Lead, COVID-19 Exposure Notification Initiative, US Centers for Disease Control and Prevention
- Dr. Viktor von Wyl, Professor, Epidemiology, Biostatistics and Prevention Institute, University of Zurich
- Dr. Louise Ivers, Professor of Medicine, Harvard Medical School; Interim Chief of Infectious Diseases and Executive Director of Center for Global Health – Massachusetts General Hospital

The 1 ½ hour panel discussion was videotaped and is available for viewing at https://www.nist.gov/news-events/events/2021/01/challenges-digital-proximity-detection-pandemics-privacy-accuracy-and. This report provides only a summary of key topics that were discussed and some of the themes that emerged.

The panel discussion began with each panelist giving their perspective on what "effectiveness" means to them, then moved on to a conversation about whether it is 'too late' for a technology like exposure notification to have an impact in the U.S. and whether we have enough data yet to know if automated exposure notification is, in fact, augmenting manual contact tracing as expected. The moderator brought a discussion among workshop participants on the Slack channel to the panelists, asking about the potential economic impact of AEN and what economic impact should be considered. The conversation then turned to perspectives on the intermingling of private companies with public health. Another topic brought to the panel from the Slack channel was the question, "What are we missing right now to make this technology more effective?" This was followed by a discussion of metrics needed to evaluate AEN. The panel finished with each panelist answering the question, "If you could go back a year in time, when you were just starting to think about these things, is there any other advice or things you would like to tell yourself?"

Some, but not all, of the key ideas that emerged over the course of the discussion included

- Effectiveness can be viewed from many different lenses, including a public health perspective (for example, does it reduce transmission?), an economic perspective (for example, is there enough impact to justify the expenditure), and a technology perspective (does the tool do what it's supposed to do, e.g. measure proximity? How quickly are people notified of exposure?).
- Public trust and messaging to the public to create that trust are key.
- It's important to understand and design around what will motivate someone to use the technology.

- The community needs more data and resources to evaluate how well AEN is working.
- Many of the apps as they are implemented today are so privacy preserving that it is difficult to obtain the data needed to evaluate the impact on mitigating the spread of COVID-19.
- Automated exposure notification is one tool that should augment the suite of tools society has to battle pandemics.
- Focusing on GAEN protocols and smartphones may be limiting the community's creativity; considering multiple approaches can help lead us to more innovative solutions.
- AEN can be a very useful tool in identifying 'cluster' exposures, which appear to be responsible for much of the COVID-19 spread. This will be useful even after vaccines are widely available.
- This technology is variant agnostic so can be used over the duration of the pandemic or even across pandemics.
- These concepts and technologies should continue to be developed and studied so that they can be useful tools in future pandemics; in doing so, it's imperative that public health experts be included in the process.

There were three polls to the audience during the panel. The poll questions and responses are listed in Table 1.

Table 1. Poll results.

Is it too late for a technology like exposure notification to make a strong impact in the US?	*Do you trust Google/Apple as a gatekeeper for exposure notification systems?*	*Should apps be opt-in or opt-out by default?*
Yes - 15% **No - 61%** **Uncertain - 24%**	**Yes - 18%** **No - 47%** **Uncertain - 35%**	**Opt-in - 56%** **Opt-out - 32%** **Uncertain - 12%**

4. Breakout Session Reports

Eight facilitated breakout sessions occurred the afternoon of January 27, labeled 1a – 1d for the first round of sessions and 2a – 2d for the second round. The topics of the sessions were informed by the results of a survey at the end of the first day of the workshop asking participants which issue were of greatest interest. Key questions asked of the groups and a summary of the discussions in these sessions are provided below.

4.1. 1a Applications of Proximity Detection

What are the different ways proximity detection can be used to limit the spread of pandemics (digital contact tracing, encounter metrics, etc.)? Which are most promising? What are other applications of exposure notification systems?

Key themes from this breakout session involved public awareness and acceptance of digital contact tracing and how that could benefit future U.S. pandemic readiness. That led to a conversation around the challenges of app adoption and the different aspects of apps that impact public acceptance of

exposure notification apps. This conversation led to a suggested action of more active research specifically in app adoption.

The discussion continued with a conversation around the definition of "proximity" and how it is affected by location (home, office, vehicle, indoors or outdoors), whether it is location-based (i.e., room or elevator) or people-based. Different notions of proximity are valuable, i.e., rather than proximity to a particular infected person, people might think of proximity in terms of a wave of infections approaching through their personal network (like long-range radar). This discussion led to a suggested action to consider how to implement these different notions of proximity such as stationary beacons or "radar" apps that allow people to see an infection three or four contacts away in their personal network (for example the NOVID app). In all of these, the privacy trade-offs need to be researched and understood.

Other points that were made in this breakout discussion included the importance of testing to identify asymptomatic cases, and the importance of making sure people are not asked to quarantine so much that they ignore the alerts and information proximity detection can provide them.

Looking towards the future, questions were asked about using data from an exposure notification app to infer the dynamics of the disease or using the flexibility of the technology to move beyond the < 2 m, > 15 minutes design specification for an infectious contact.

4.2. 1b Privacy (part 1) and 2b Privacy (part 2)

How are privacy risks generated by proximity detection technologies understood and managed?

What are the greatest challenges to achieving strong privacy properties while delivering effective proximity detection? How can privacy gains or losses be understood with different implementations?

The following is a summary of the questions and topics discussed by participants during the two privacy breakout sessions.

- *What are the privacy risks generated by proximity detection/contact tracing applications?*

  Participants discussed that there are already 500+ vendors of technology for some aspect of digital proximity detection, and nearly all their solutions live on smartphones. Smartphones actively collect data from users, sensor data, and connect to other devices. It is not clear if all vendors will adhere to boundaries that protect user privacy now or even going forward. It is unclear whether vendors should be trusted to prioritize patient privacy. A "Put your trust in us, think about the effects later" approach seems unreasonable.

- *Smartphones are/can be surveillance tools. To avoid adding apps for public health to these platforms, what alternative technologies can be used?*
  Participants suggested alternative options including dongles or wearables, and the approach of using beacons. Some suggested that future efforts should use scientific principles to guide the approach to proximity-detection technology instead of relying on the existing "pocket power" of phones. The community may be limiting itself by focusing on an existing technology that wasn't specifically designed with public health and scientific data collection in mind.

- *What are barriers to separating AEN apps from smartphones?*
  Participants expressed concerns that "big techs" has the "pocket power" – smartphones have infiltrated our lives, to the point that we carry smart phones around constantly, and questioned whether any other technology can achieve the level of adoption of smartphones. Participants noted that some people may not understand that alternative technology may be necessary, may not view phones as intrusive, lacking awareness of the potential risks of relying on infrastructure operated by big tech.

- *Public health infrastructures are massively underfunded, private infrastructures are overfunded. How can we achieve better balance*?

  There seemed to be consensus from session participants that the imbalance exists, and there is no clear path to a better balance. They identified factors contributing to the imbalance including a lack of public awareness and understanding. Again, participants expressed concern that collecting data on private platforms creates a dependency on the private companies going forward, and it is unknown how the rights and usage to the data they collected would be governed.

- *Does the public understand the risks around losing privacy? Do we have a consensus on the definition of privacy?*
  Participants stated that the definition of privacy seems to be context dependent. For example, the public does not often want to deal with the efficiency loss found in privacy-centric solutions. Many people, including the highly educated, don't understand the argument for privacy. There is a sense of apathy ("all our data is already out there, what's the big deal?"), and people do not understand the risks. Session participants noted that explaining the risk is challenging.

- *Should technologists seek guidance on how to agree on one definition of privacy from those who regularly work on privacy-related definitions (lawyers, etc.)?*
  This question was debated, with no clear consensus.

- *Is the public health perspective on proximity-detection technology almost contrary to the privacy perspective?*
  Participants discussed the morning's panel session, during which speakers had noted that the privacy-preserving features of the GAEN service result in data that aren't useful for public health officials. To address this, some participants noted that if phone companies allowed developers greater access to the lower level real-time operating systems of the smartphones, then desirable features like cryptography could be embedded that allow public health professionals to obtain the information that's helpful to them in a way that doesn't reveal any individual-level information. Some of the technologists/engineers in the session said they would like to know what (data) exactly the public health officials need so they can create a system that would only offer this data without revealing any additional data. They stressed that designers want to prevent any additional inferences from being made, perhaps even at a later time. To make sure the data from the apps are valuable data for public health reasons, one must ensure the users are educated properly to know how to use the technology to ensure the data collected is clean. Using production data as scientific data can be problematic because, for example, little to nothing may be known about the conditions under which the data was acquired.

- *Should privacy be the end goal?*
  Beyond the app, breakout session participants discussed the next steps/full ecosystem that involve(s) user data (call center employees, call center databases, etc.). One participant noted that autonomy is a bigger personal goal than privacy, citing the article:
  Proximity Tracing in an Ecosystem of Surveillance Capitalism, https://arxiv.org/abs/2009.06077v1.

- *Privacy is not binary. There is no "on/off" switch. Thoughts?*
  Participants discussed that the public often does not know what they are signing up for despite access to long privacy agreements and talked about the differences between voluntarily seeking medical intervention and requiring public health intervention. Some noted an irony in what users already disclose to smartphones/websites vs. the deep concern specifically about contact tracing apps. Participants also noted that in terms of community building/trust building, challenges differ between different populations and the reasons why people care about privacy vary. Lack of understanding of technology may lead the public to believe that layering a new technology onto existing technology will safeguard privacy when, in fact, it might not.

- *Privacy needs of employees in the workplace: how can proximity detection in a workplace work while also protecting the privacy of employees?*
  Session participants discussed using a beacon approach to detect when persons are within close proximity of the beacons, instead of detecting when persons are close to each other. Some participants stated that the hardware options are fairly cheap, but it can be difficult for companies (business customers, employers, etc.) to understand what vendors are actually offering (wearables, GAEN, etc.), and what their choices are for navigating the pandemic. Also, the sessions' participants discussed what policies might be needed, for example will data be destroyed after the pandemic is over? How will the data be used post-pandemic? The group noted that policies to protect data after the pandemic would be helpful.

- *How can NIST help?*
  Several suggestions for what NIST can do were offered, including to run a competition on privacy-preserving proximity tracking & standardize a solution, as well as developing new (advanced) cryptographic techniques. The participants noted that new standards could lead to more accessible explanations of these techniques, which would lead to (hopefully) better understanding throughout the general population. Other participants suggested that NIST could work with other groups like Bluetooth SIG. Finally, some of the session participants suggested NIST could create communication about privacy advocacy (NIST is restricted from affecting the markets, advancing the profitability of individual companies) that would be accessible for a general audience, but noted that some stakeholders would likely not benefit from this.

4.3. 1c Technologies for Proximity Detection

How accurately can different technologies identify a contagious interaction? How can machine learning (ML) be used for signals/sensors other than the BLE (e.g., ultrasound, lidar)?

The participants of this session identified many technologies (not limited to smartphones) that could be used for proximity detection. These include ultra-wideband to allow more accurate ranging between 2 radios and through walls; ultrasound to allow potential for 3 cm ranging accuracy that would confirm people are in the same air space; Bluetooth; lidar; triangulation or history of activity/location; infrared; Wi-Fi; barometers; CCTV; inertial sensors; cameras; and microphones that use data bursts to compare and preserve privacy. They saw a potential in using sensor fusion to reduce false positives, i.e., multi-sensor technologies could enhance validation.

The group went on to discuss that shared air and typically indoor air is how the virus is transmitted between people. A different algorithm for detecting an infectious contact may be needed for different applications (e.g., manufacturing or meatpacking compared to the public). The group identified ventilation as a concern, noting that sensors could be used to determine airflow characteristics and relative humidity, and artificial intelligence (AI)/ML could be used to indicate potential infection events.

The theme of a need to define the specification better (distance, time accumulation and duration, strength of viral load) came up in this discussion, as it did in many other discussions during this workshop. Participants stressed that the technology should identify likelihood of transmission, not necessarily just proximity.

When asked what researchers need to proceed, participants agreed that data that could be used to develop solutions was lacking. For example, are there data/characteristic proxies for virus load; could smoke be used as a proxy for airborne virus load? Carbon Dioxide may be a proxy to describe the air (unless scrubbers employed). Large amounts of data would help for construction of AI learning data sets, but current analytics are limited due to size of data sets, accuracy of the data, and compatibility. The participants wondered whether researchers could partner with existing commercial applications and existing location/networking data to gather data sets. They also asked whether there is ground-truth data that is needed that is not yet accessible that may be more private and agreed that a data toolbox for future pandemic analysis would be helpful.

Other technologies that were mentioned during the session included chemical analysis via mobile devices, a virus analogue of insect/animals that can detect biological signatures, plug-in devices that could extend sensor/phone capabilities, and air-space characteristics monitored via fixed sensors in each room or building with data transmitted to a cloud service or device and processed for alerts.

4.4. 1d Role of Government

What role should local, state, and federal government play in digital contact tracing?

Continuing a recurring theme in the workshop, the first concern was around privacy vs. health concerns. Where and when should we prioritize protecting the individual vs. community-at-large? How do we work within HIPAA law? Participants suggested that

Federal-level guidance on what HIPAA covers, to reduce misinterpretations of law/policy, would be helpful.

Another topic of concern raised by session participants was the lack of documentary standards. They noted that technical standards might help to level the playing field for different organizations, looking to GAEN as an example of a system that was set up without the context of agreed-upon standards. The group discussed NIST as convener of resources and stakeholders to facilitate standards development (NIST is not a regulatory agency and does not write documentary standards, although NIST technical staff are involved in the development of standards). Two issues around standards identified by participants were the long timeline (e.g. the timeline for developing standards is typically years, so while useful for future pandemics, they may not address current concerns) and the reality that standards development and standards participation in the U.S. is voluntary.

Participants identified that NIST could also facilitate a broader audience to create protocols and build out communication with other stakeholders to develop robust solution platforms. This engagement could also create opportunities for collaboration by bringing stakeholders together. Another activity the government might undertake could be creating tools for governments to better understand and deal with decisions for contact tracing systems. Some participants felt the federal government should take a larger role in procedures and standards and communicating federal-level statutes more clearly to state and local governments.

Should there be a Federal Contact Tracing App in the U.S.?

The group asked whether the U.S. should implement a federally coordinated app because it might be more broadly used and could be consistently regulated. Advantages identified by the session participants included that Federal resources could be brought to bear to develop momentum, while local governments may lack resources beyond adoption and communication, and it could allow roles and responsibility to be parsed out to respective government groups best suited to assist. Further, some noted that an app is monopolist by nature. The group also noted that significant trust and privacy concerns among the public would likely persist even in the federal app scenario.

4.5. 2a Implementation/Public Acceptance

What adoption rate is needed to be effective in different communities? What are the barriers to adoption and use, and how should they be addressed? Should the public be encouraged to adopt existing apps? What strategies should be used to encourage adoption? What are the roadblocks to greater adoption and how can they be removed?

The participants identified the following barriers to adoption:

- Trust
- Hesitancy to change current behaviors, where current behaviors are not participating in an app; unwillingness to adopt a new program
- Fear (of a false positive notification; lots of questions or uncertainty surrounding a notification of exposure)
- Already encountering COVID every day, so what benefit could there be?
- Can't afford quarantine (so then no desire to know if exposed and should quarantine)
- Equity: barriers specific to each community or fears specific to a group

- Knowledge of the app, awareness of the app (rather than not wanting to use it)
- False information or misinformation
- Political messaging, conflicting messaging from government, changing messages
- Opt-out v. opt-in (requires more personal energy if it is opt-in rather than opt-out)
- Personal benefit: the act of installing the app doesn't personally reduce infection risk (rather, installing the app increases risk of cost of quarantine)
- Technological readiness (is the user capable of installing, using an app; willing to try a new app)

The participants had the following suggestions to help overcome these barriers:

- Need to communicate the personal advantage, the personal benefit, the value proposition
    - What's the cost? This could be privacy (tracking, supplying personal info), battery use or many of the other barriers identified above
    - The value proposition needs to overcome these potential costs
    - Perceived benefits drive more adoption, rather than privacy concerns preventing adoption
    - Once you have a certain percentage of uptake in a community (can be a small community group), then you get personal benefit
- Trust
    - Need unified, well-crafted messaging *at the 6th grade level*
    - Overcoming misinformation
    - Understand the relationship between the public and an entity that can convince people to download. In some places, e.g., United Kingdom, the NHS fills that role. Is there such an entity in the U.S.?
- Awareness of the app
    - Need marketers and influencers to reach the community
    - Does the adoption rate increase when persons know other people that have adopted it?
    - Does a user download the app if it makes them feel part of their community?
- Ideas for user engagement, which can contribute to personal benefit, trust, and a goal of making others aware of the app
    - How "effective" is the app?
    - What benefits were there to the community by participating?
- Will GAEN apps make a difference in the U.S.?
    - Even if we have large adoption, will it make a *positive* difference?
    - Will people have negative memories of the app (e.g., too many notifications, too many false positives)?
    - Should we be changing something now to prevent negative impacts?

4.6. 2c Technology Evaluation and Verification

What is needed to verify the performance of proximity detection technologies? What are the barriers to verification? Are standards needed, and if so which ones? For machine learning evaluation, what data sources are needed for reliable training and evaluation?

Participants had a robust discussion, noting that to verify the performance of proximity detection technology, one needs to simulate the complicated, real-world environment so that scientists can investigate how measurements correlate with the real risk factors for real

people in the real world. It's important to consider mobility by including both static and mobile test cases. Interference must also be considered. One way is to log corresponding frequencies when gathering signal data associated with multiple channels, for example, BLE uses channels 37, 38, and 39 for broadcasting. Crowd-sourced experiments that test scenarios in which people are doing normal business naturally would be very useful. The group debated issues around using robots vs. humans to gather data. Robots facilitate extensive data collection, but the existence of people might affect the results, and it's hard for robots to mimic all types of human poses and behaviors.

To tackle the issue of different infection risks at the same distance due to different interaction behaviors (for example, no talking, shouting, separated by walls), the group discussed adding other sources of data to evaluate risk, such as duration/contact time and interaction types. Ways to discriminate whether the interaction occurs indoors or outdoors using smart phones include checking light sensors, light fluctuations in the camera, amount of visible Wi-Fi access points, amount of visible cellular cells, number of GPS signals and their strength. Area statistics such as room size, ventilation, and room number that could be emitted by broadcast-only devices might help to determine the severity of contact; such information needs to be associated with additional information that is specific enough to evaluate possible infectious interactions. Participants noted that data are lacking for RF signals between phones/devices (they might not be static during measurement and will be held and located in different ways). With all these options, the group stressed that privacy remains a consideration.

To verify performance, the group emphasized that strong multi-disciplinary collaborations are needed.

The group also asked about standards. Do we need standards for evaluation and verification, or for the technologies? Aspects identified by the group that should be covered in the standards include a definition of a contact or exposure, interoperability, privacy, how the phone/device gathers and exchanges information, how the phone/device stores and destroys the data, a common way of calculating the exposure risk based on contacts, their duration, distance, environment, etc.

To support machine-learning applications, researchers and developers need richer real-world data sets, data sets with high precision, data sets that use signals of higher bandwidth

The group stressed that the underlying hardware should remain inexpensive and available at the national scale.

4.7. 2d Future Context

How can technology help prepare us for the next pandemic? What work still needs to be done? What unintended consequences of using proximity detection technologies need to be addressed and how?

The participants first took a broad view of technology and discussed technology beyond contact tracing in the context of helping us prepare for the next pandemic. Technology for better testing; a capacity for scaled up testing rapidly and early was mentioned. Technologies for research to better understand how intervention approaches impact the spread of disease was discussed. This impacts what technology approaches are used for which diseases (e.g. airborne vs. other modes of transmission). Technology systems that can handle disease more

infectious than COVID-19 may be needed. More studies and data to verify will be required. One possibility is to use tech to mimic disease spread. Perhaps tech can be used for 'pandemic fire drills' to practice response, the way we do for other scenarios. Always-on mobility tracing could be used to more quickly detect when a new pandemic breaks out.

Next, the participants discussed technology for better communication with the public. They touched on the recurring theme throughout the workshop of consistent and timely messaging, translating technical results into plain language for public consumption, and messaging for prevention. They also touched on a recurring theme throughout the workshop around the messaging to emphasize individual risk/benefit. Specific ideas included engaging social media influencers to help get the message out and providing open Q&A sessions in local communities.

The discussion then turned to the questions around what work still needs to be done, what unintended consequences of using proximity detection technologies need to be addressed and how, and what else we should be thinking of for the future of digital proximity detection. First, the infrastructure now in place must be maintained to avoid reinventing the wheel. New infrastructure could be put in place, for example pandemic-resistant buildings with better ventilation design and/or virus detectors akin to smoke detectors, standard wastewater testing, or infrastructure that helps people remain safely at home when an aggressive stay-at-home order is required.

Another recurring theme throughout the workshop was the idea of beacons designed to augment digital proximity detection with additional data. This group also discussed the concept, suggesting that they be placed in popular locations such as buses or restaurants. They pointed out that this can be powerful, because multiple parties don't have to install an app. This infrastructure should also be in place beforehand, including possibly in private gathering spaces like churches. The beacon idea could possibly be expanded for air quality or wastewater application. However, one must consider the ownership of this infrastructure. If it is under the control of for-profit organizations, what does this mean? The group discussed whether networks like FirstNet, a dedicated interoperable communications network for first responders, could provide lessons learned.

Other issues raised by participants included:

- Issues of equity and efficacy, especially if solutions are tied to ownership of smartphones. How can all demographics be considered, including the "edge cases?" Researchers and developers should ask themselves how they can be intentional about including all groups. Children are also an important and underrepresented group.
- To future-proof, we need to think ahead. How can the technology be platform/tech-agnostic? What will we carry ubiquitously in the future? Wearable/embedded tech? Consider threats of bioterrorism and how we might address future customized virus creation.
- The need for measurements and data to show how well apps are really working, echoing a recurring theme throughout the workshop. Metrics must be captured in a privacy preserving way. Public health experts must be involved. Data will likely need to be integrated from multiple sources.
- Finally, the participants touched on another workshop theme – the need to address low adoption rates by improving and simplifying the user experience, identifying and

speaking to the value proposition for the individual user, and addressing privacy concerns (noting that HIPAA clarification would be useful).

5. Contributed Talks

Thirteen, ten-minute contributed talks were presented on Thursday, January 28. These talks addressed the speakers' research and ideas into more specific topics. The content varied widely, from new ideas on the use of beacons privacy, machine-learning applications and additional TC4TL data analysis, modeling for vulnerable communities, and cluster event exposure notification without proximity detection to multipath interference for BLE scoring, testbeds, data fusion of mobile sensors and alternate paradigms for digital contact tracing. Some of the speakers' presentations can be found on the workshop website: https://www.nist.gov/news-events/events/2021/01/challenges-digital-proximity-detection-pandemics-privacy-accuracy-and.

6. Summary

This three-day workshop addressed challenges for digital proximity detection in pandemics. Experts from a variety of different fields shared their ideas and opinions. Key themes and some of the recommended actions have been summarized in the executive summary.

Appendix A: Acronyms

AEN	Automated Exposure Notification
AI	Artificial intelligence
API	Application Programming Interface
BLE	Bluetooth Low energy
DPD	Digital Proximity Detection
GAEN	Google/Apple Exposure Notifications
HIPAA	Health Insurance Portability and Accountability Act
MIT	Massachusetts Institute of Technology
ML	Machine learning
NIST	National Institute of Standards and Technology
PACT	Private Automated Exposure Notification
TC4TL	Too Close for Too Long

Appendix B: Agenda

Workshop on Challenges for Digital Proximity Detection in Pandemics: Privacy, Accuracy, and Impact

Jan. 26 – 28, 2021

https://www.nist.gov/news-events/events/2021/01/challenges-digital-proximity-detection-pandemics-privacy-accuracy-and

Tuesday, January 26, 2021 All times are Eastern Standard Time (EST)

10:00 am	Welcome and Opening Remarks
10:10 am	*Who should you be talking to? 3 lessons in interdisciplinary problem-solving* Joanna Masel, Professor, Department of Ecology & Evolutionary Biology, University of Arizona A critical look at exposure notification through the lens of its end-goal – fighting the pandemic – reveals a variety of pitfalls in interdisciplinary problem-solving. For example, assuming that problems in disciplines other than your own are already solved can lead to overly narrow design specifications, such as classification with respect to 6-foot 15-minute thresholds rather than estimation of infection risk. Strategies for extracting information from other disciplines, and indeed for discovering the existence of relevant disciplines in the first place, will be discussed.
10:55 am	*A Brief Tutorial on Private Automated Exposure Notification for COVID-19* Marc Zissman, Associate Head, Cyber Security and Information Sciences Division, Lincoln Laboratory, Massachusetts Institute of Technology Beginning early in the pandemic, international teams of cryptographers, electrical engineers, physicians, computer scientists, public health professionals, privacy experts and other specialists proposed approaches to automate the process of detecting potential exposure to COVID-19-infected individuals using Bluetooth signaling on smartphones that could supplement conventional, manual contact tracing (MCT). The value proposition had four components: automated exposure notification could lead to faster alerting and action vs MCT alone, could reach persons who are not personally known to an index case, could continue to function even when MCT reaches resource limits or breaks down, and could provide alerts while protecting privacy. Influenced to some extent by the work of these international teams, Apple|Google developed an automated exposure notification system based in part on the protocols and prototypes developed and demonstrated by these international teams. A|G deployed that system quickly and widely, and the system is now in use in over 30 nations and US states, has been enabled via user opt-in on tens of millions of smartphones, and has provided hundreds of thousands of exposure notifications to close contacts. To varying extents, all four elements of the value proposition have been proven – the system works. In this talk, the overall approach to private, automated exposure notification is explained, with emphasis on the operation and performance of all three layers: Bluetooth-based proximity measurement, the private cryptographic protocol, and the public health / individual user interfaces. Preliminary estimates of both performance and effectiveness from deployments around the world are discussed.
11:25 am	Transition

11:28 am	*Real-world effectiveness of digital contact tracing* Luca Ferretti, Senior Researcher in Statistical Genetics and Pathogen Dynamics at the Big Data Institute, University of Oxford After many countries deployed apps for proximity detection and exposure notifications, there is still a lack of understanding of their potential and actual impact. In this talk we review the theoretical expectations about the potential impact of app-based contact tracing, and we discuss the main known and unknown factors that affect its effectiveness. Then, we discuss the role of these factors and the actual impact of such apps in some European countries.
11:50 pm	Break
12:20 pm	Transition/introduction of speakers
12:25 pm	*The SwissCovid GAEN app after six months: It's not just about technology.* Viktor von Wyl, Assistant Professor, Epidemiology, Biostatistics and Prevention Institute, University of Zurich The SwissCovid app was released in Switzerland as one of the first GAEN apps on June 25, 2020. This presentation will briefly recap the challenges for measuring effectiveness in a highly decentralized health system, the state of evidence for effectiveness, as well as lessons learned. Ultimately, the success of GAEN apps not only depends on technological aspects but also on appropriate health system embedding and engagement by different actors.
12:47 pm	*Public acceptance of emerging technologies* R. Alta Charo, Knowles Professor Emerita of Law & Bioethics, University of Wisconsin Madison This presentation will describe some experiences in the past with public reaction to new technologies and identify measures that can be taken to increase enthusiasm, decrease concern, and substantively address risks.
1:09 pm	*Public health perspective of digital contact tracing in COVID-19 using Bluetooth-enabled technology* Meghna Patel, Deputy Secretary for Health Resources and Services, Pennsylvania Department of Health The spread of COVID-19 in the communities is so overwhelming across the globe that the ability to track, trace, isolate and test the individuals suspected to have the virus is impossible without the influx of additional staff and use of technology assisted applications. Traditional contact tracing is unable to account for contact with individuals unknown to the person who tested positive (e.g., an individual who tested positive cannot name others he/she rode the bus with). Bluetooth-enabled technology is a promising solution to assist with exposure notification where traditional contact tracing cannot. It is important that guiding principles of data privacy remains at the core when implementing a technology- assisted exposure notification. These applications will be effective if priority for testing is established or mass testing is available or both as well as massive campaign focusing on trust. As the future of public health becomes more led by technology to help stop the spread of infectious diseases, there are several limitations to implementing and sustaining digital contact tracing technology solutions.
1:31 pm	Break
1:40 pm	Transition/introduction of speakers
1:45 pm	*Privacy considerations, an overview*

	Naomi Lefkovitz, Senior Privacy Policy Advisor, Information Technology Lab, NIST Management of privacy risks, whether real or perceived, is a key factor in successful adoption of large-scale pandemic technology solutions. This presentation provides an overview of some of the privacy considerations for proximity detection technologies, including considerations for assessing tradeoffs with effectiveness, usability, security, and different implementation environments.
2:07 pm	*Privacy preserving protocols for encounter metrics* Rene Peralta, Computer Scientist, Cryptographic Technology Group, NIST We propose measuring aggregate levels of encounters in a population, a concept we call "encounter metrics". Our proposal is to design encounter metrics in such a way that it can be deployed while preserving the privacy of individuals. To this end, our proposal is to label encounters with a random number (an encounter ID) that cannot be linked to anything that is broadcast at the time of the encounter. This mitigates significant privacy concerns inherent to methods that broadcast and track user pseudonyms instead of encounter IDs. Encounter metrics can be used to analyze the interactions within populations as we attempt to safely restart our societies during the pandemic of 2020. The aggregate encounter metric statistics will facilitate analysis of population interactions in buildings, comparisons across buildings or campuses, and data-driven adjustments in reopening processes. These measurements will also be valuable in designing our future working environments to be more resilient to spread of infectious diseases.
2:19 pm	*Privacy by Design as Infrastructural Power* Seda Gürses, Associate Professor, Department of Multi-Actor Systems at TU Delft During this talk, I will give an overview of the series of events that led to and followed from the development of the Decentralized Privacy Preserving Proximity Tracing (DP3T) protocol that underlies the Google Apple Exposure Notification (GAEN) API. Underlying engineering efforts in privacy by design is the assumption that data control and data minimization will enable the protection of individuals and therewith mitigate the growth of power asymmetries. The GAEN story, however, suggests that data minimization, a guiding design principle for engineers and privacy advocates, may not always come to tame power. On the contrary, the infrastructural advantage that companies like Google and Apple possess allows them to leverage privacy enhancing protocols to expand their reach. This has serious repercussions both for privacy by design as well as the democratic governance of technologies for public use, matters pertinent to reflect on given the increasing number of applications for population management using digital technologies.
2:41 pm	Transition/introduction of speakers
2:45 pm	*Flipping the Perspective on Contact Tracing* Po-Shen Loh, Founder of NOVID, Professor of Mathematical Sciences at Carnegie Mellon University, and National Coach of USA International Math Olympiad team We introduce a fundamentally different paradigm for contact tracing, enabled by the proliferation of smartphones: for each positive case, do not only ask direct contacts to quarantine; instead, tell everyone how many relationships away the disease just struck (so, "2" is a close physical contact of a close physical contact). This new approach,

	which has uniquely been deployed in the publicly downloadable app NOVID, brings a new tool to bear on pandemic control, powered by network theory. Like a weather satellite providing early warning of incoming hurricanes, it empowers individuals to see transmission approaching from far away and becomes the first proximity detection app whose installation reduces the user's own chance of infection. This flipped perspective incites natural self-interested instincts of self-preservation, reducing reliance on altruism, and the resulting caution reduces pandemic spread in the social vicinity of each infection. Consequently, our new system solves the behavior coordination problem which has hampered many other app-based interventions to date. Indeed, from the game-theoretic perspective of Nash Equilibria, standard apps unfortunately only reach equilibrium when nobody installs, whereas our approach is also at equilibrium when everybody installs. In addition to this, our approach has 3 order-of-magnitude power gains over the status quo.
3:07 pm	*Machine learning based digital proximity detection: lessons learned from the NIST TC4TL Challenge and beyond* Omid Sadjadi, Computer Scientist, Information Technology Lab, NIST The NIST pilot Too-Close for Too-Long (TC4TL) Challenge, which was conducted in the summer of 2020 in response to the COVID-19 pandemic, was a machine learning challenge to explore promising new ideas in, and evaluate the efficacy of, digital proximity detection based on Bluetooth Low Energy (BLE) and other smartphone sensor data. This talk will provide an overview of the TC4TL challenge, including descriptions of the task, datasets, performance measure, participation statistics, as well as results and system performance analyses. Some potential avenues for future work will also be presented and discussed.
3:30 pm	Adjourn

Wednesday, January 27, 2021 All times are Eastern Standard Time (EST)

10:00 am	Panel discussion on the *effectiveness of digital proximity detection at limiting the spread of infectious diseases.* This panel will discuss questions such as *How should we define 'effective'? How do we know models showing proximity detection effectiveness are right? How does the implementation and effectiveness change for different sizes and types of communities?* Krister Shalm (moderator), Applied Physics Division, NIST and Physics Department, University of Colorado, Boulder Marc Zissman, Associate Head, Cyber Security and Information Sciences Division, Lincoln Laboratory, Massachusetts Institute of Technology Po-Shen Loh, Founder of NOVID, Professor of Mathematical Sciences at Carnegie Mellon University, and National Coach of USA International Math Olympiad team Mike Judd, Lead, COVID-19 Exposure Notification Initiative, US Centers for Disease Control and Prevention Viktor von Wyl, Professor, Epidemiology, Biostatistics and Prevention Institute, University of Zurich

	Louise Ivers, Professor of Medicine, Harvard Medical School; Interim Chief of Infectious Diseases and Executive Director of Center for Global Health – Massachusetts General Hospital			
11:30 am	Instructions for breakout sessions			
11:40 am	Break			
	Breakout Sessions			
12:00 pm	1a *Applications of proximity detection* *What are the different ways proximity detection can be used to limit the spread of pandemics (digital contact tracing, encounter metrics, etc.)? Which are most promising? What are other applications of exposure notification systems?*	1b *Privacy 1* *How are privacy risks generated by proximity detection technologies understood and managed?*	1c *Technologies for Proximity Detection* *How accurately can different technologies identify a contagious interaction?*	1d *Role of government* *What role should local, state, and federal government play in digital contact tracing?*
	Facilitator: Leah Kauffman	Facilitator: Jessica Staymates	Facilitator: Ashley Boggs	Facilitator: Brandi Tolliver
1:30 pm	Break			
2:00 pm	2a *Implementation* *What adoption rate is needed to be effective in different communities? What are the barriers to adoption and use, and how should they be addressed? Should the public be encouraged to adopt existing apps? What strategies should be used to encourage adoption? What are the roadblocks to greater adoption and how can they be removed?*	2b *Privacy* *What are the greatest challenges to achieving strong privacy properties while delivering effective proximity detection? How can privacy gains or losses be understood with different implementations?*	*2c Technology evaluation and verification* *What is needed to verify the performance of proximity detection technologies? What are the barriers to verification? Are standards needed, and if so which ones? For Machine learning evaluation, what data sources are needed for reliable training and evaluation?*	2d *Future Context* *How can technology help prepare us for the next pandemic? What work still needs to be done? What unintended consequences of using proximity detection technologies need to be addressed and how?*
	Facilitator: Jeanita Pritchett	Facilitator: Jessica Staymates	Facilitator: Callie Higgins	Facilitator: Jeremy Lawson

Thursday, January 28, 2021 All times are Eastern Standard Time (EST)

10 am	Reports from working groups (10 minutes each) Moderator: Heather Evans, Program Coordination Office, NIST
11:30 am	Contributed Talks Moderator: Michelle Stephens, Applied Physics Division, National Institute of Standards and Technology

	Privacy-Protecting COVID-19 Exposure Notification Via Cluster Events Without Proximity Detection, Paul Syverson, U.S. Naval Research Laboratory *Augmenting GAEN with opt-in case linking*, James Petrie, WeHealth *Adoption metrics for Proximity Technologies,* Scott David, Director of Information Risk Research Initiative (IRRI), University of Washington Applied Physics Laboratory *Modeling the impact of automatic exposure notification for vulnerable communities* Krister Shalm, Applied Physics Division, NIST and Physics Department, University of Colorado Boulder *Understanding and Rewiring Epidemic Networks: A Data-driven Approach Towards Enabling Quarantine in-Motion*, Radu Marculescu, Department of Electrical & Computer Engineering, The University of Texas at Austin
12:30pm	Break
1:00 pm	Contributed Talks/Discussion Moderator: Michelle Stephens, Applied Physics Division, National Institute of Standards and Technology *Interoperable Privacy Preserving Digital Contact Tracing*, Yang Yaling, Virginia Tech *Function Secret Sharing for PSI-CA: With Applications to Private Contact Tracing*, Steve Lu, Stealth Software Technologies, Inc. *Modelling multipath interference for BLE proximity detection and exposure scoring*, Ramsey Faragher, CEO Focal Point Positioning, Fellow in Computer Science, Queen's College, University of Cambridge *COSMOS Testbed – Proximity Detection and Social Distancing Estimation in COVID-19 Pandemic*, Zoran Kostic, Electrical Engineering Dept., Columbia University *A Simplistic Machine Learning Approach to Contact Tracing,* Niamh Belton, ML-Labs, University College Dublin *The Feasibility of Co-location Detection through a Deep Learning Fusion of Mobile Sensors*, Sheshank Shankar, Data Science Researcher, PathCheck Foundation *Entropy Based Discretization's and Weight Optimization for Configuring the GAEN system*, Nicholas Maynard, The MITRE Corporation *Efficacy of Current Approaches and An Alternative Paradigm for Digital Contact Tracing*, Brian Thompson, MITRE Corporation
2:36 pm	Break
2:45 pm	Discussion and Summary Moderator: Heather Evans, Program Coordination Office, NIST
3:30 pm	Adjourn