National Committee on Vital and Health Statistics Hearing on Privacy, Confidentiality, and Security Considerations for Data Collection and Use during a Public Health Emergency

Transcript

September 14, 2020, 9:30 a.m. – 5:15 p.m. ET

VIRTUAL

SPEAKERS

NCVHS Members		
Name	**Organization**	**Role**
Frank Pasquale	**University of Maryland Carey School of Law**	**Chair**
William W. Stead	**Vanderbilt University**	**Chair, Full Committee**
Rebecca Hines	**NCHS**	**Executive Secretary**
Denise Chrysler	University of Michigan School of Public Health	Member
Jacki Monson	Sutter Health	Member
James J. Cimino	University of Alabama at Birmingham	Member
Jamie Ferguson	Kaiser Permanente	Member
Melissa M. Goldstein	The George Washington University	Member
Nicholas L. Coussoule	BlueCross BlueShield of Tennessee	Member
Richard W. Landen	Individual	Member
Vickie M. Mays	UCLA	Member
Wu Xu	University of Utah	Member
NCVHS Staff		
Name	**Organization**	**Role**
Rachel Seeger	HHS Office for Civil Rights	Lead Staff
Maya Bernstein	ASPE/OSDP	Staff
Geneva Cashaw	NCHS	Staff
Marietta Squire	NCHS	Staff
Presenters		
Name	**Organization**	**Role**
Ashkan Soltani		Independent Researcher

Commissioner Allison Arwady	Chicago Department of Public Health	Commissioner
Robert Grossman	University of Chicago	Chief Research Informatics Officer, Biological Sciences Division
Danielle Allen	Harvard University	Professor
John W. Loonsk, M.D.	John Hopkins University	Professor
Kate Goodin	Tennessee Department of Health	Director, Surveillance Systems and Informatics Program, Communicable and Environmental Diseases and Emergency Preparedness
Stacey Mondschein Katz, Esq.	Maine Department of Health and Human Services	Director of Healthcare Privacy and Human Protections Administrator
Bryant Thomas Karras, M.D.	Office of the State Health Officer, Washington State Department of Health	Chief Informatics Officer
Mary L. Gray	Microsoft Research	Senior Principal Researcher
Sean Martin McDonald	Centre for International Governance Innovation	Senior Fellow
C. Jason Wang, MD, PhD	Center for Policy, Outcomes and Prevention, Stanford University	Director

Welcome and Roll Call

Rebecca Hines: Well, good morning, everyone, and welcome to the National Committee on Vital and Health Statistics, NCVHS, meeting of the Subcommittee on Privacy, Confidentiality and Security. I hope everyone is staying safe and well.

My name is Rebecca Hines. I serve as the executive secretary and designated federal officer for the committee. Today, the committee will be hearing testimony regarding privacy, confidentiality, and security considerations for data collection and use during a public health emergency. We are grateful to our guest speakers invited here today to give input to the committee as it works to develop methods and approaches for handling data responsibly during pandemics such as the one we are in.

Before we get started, take care of our roll call duties. Please remember to state your name, the organization you are with and your role on the committee and any conflicts beginning with the chair of the subcommittee, Frank Pasquale.

Frank Pasquale: Thanks very much, Rebecca. My name is Frank Pasquale. I am chair of the Subcommittee on Privacy, Confidentiality and Security and a member of the Full Committee and no conflicts.

Rebecca Hines: Bill Stead.

Bill Stead: Hi. This is Bill Stead. I am chair of the Full Committee. I am from Vanderbilt University Medical Center and I have no conflicts.

Rebecca Hines: Denise Chrysler.

Denise Chrysler: Hi. I am Denise Chrysler. I work with the University of Michigan School of Public Health. I am with the Network for Public Health Law. I am a member of the Full Committee. I also serve on the Subcommittee on Privacy, Confidentiality and Security. I have no conflicts.

Rebecca Hines: Jacki Monson.

Jacki Monson: Good morning. Jacki Monson. Sutter Health. A member of the Full Committee and a member of the Subcommittee on Privacy, Confidentiality and Security and no conflicts.

Rebecca Hines: Jamie Ferguson.

Jamie Ferguson: Good morning. Jamie Ferguson, Kaiser Permanente, member of the Full Committee, member of the Standards Subcommittee, no conflicts.

Rebecca Hines: Jim Cimino.

Jim Cimino: Hi. Jim Cimino. University of Alabama Birmingham, member of the Full Committee, member of the Subcommittee on Standards, no conflicts.

Rebecca Hines: Melissa Goldstein.

Melissa Goldstein: Good morning. I am Melissa Goldstein. I am on the faculty at George Washington University. I am a member of the Full Committee and also a member of the Privacy, Confidentiality and Security Subcommittee and I have no conflicts.

Rebecca Hines: Nick Coussoule.

Nick Coussoule: Good morning. I am Nick Coussoule with BlueCross BlueShield of Tennessee, member of the Full Committee, the Privacy, Security and Confidentiality Subcommittee and the Standards Subcommittee. I have no conflicts.

Rebecca Hines: Rich Landen.

Rich Landen: Good morning. Rich Landen. No affiliation. A member of the Full Committee, co-chair of the Subcommittee on Standards, no conflicts.

Rebecca Hines: Wu Xu.

Wu Xu: My name is Wu Xu. Adjunct faculty for University of Utah. I am a member of the Full Committee. I have no conflicts.

Rebecca Hines: Vickie Mays.

Vickie Mays: Good morning. I am with the University of California Los Angeles. I am a member of the Subcommittee. I am a member of the Full Committee. And I have no conflicts.

Rebecca Hines: Are there any other members that I have missed? Okay. Let us turn it over to our lead staff. Rachel Seeger.

Rachel Seeger: Rachel Seeger, HHS Office for Civil Rights and lead staff to the Subcommittee on Privacy, Confidentiality and Security.

Rebecca Hines: Maya Bernstein.

Maya Bernstein: Good morning. I am Maya Bernstein. I work in the Office of the Assistant Secretary for Planning and Evaluation. I am lead staff to the executive director of the Committee and a liaison to the Subcommittee.

Rebecca Hines. Great. Thanks, all. And I just want to acknowledge our two committee staff, Marietta Squire and Geneva Cashaw. I believe that is the end of roll call. I just wanted to say that before we get started, there will be a public comment period later this afternoon. It is on the agenda for 3:45 p.m. Eastern and we will do our best to start then if you plan to speak during that public comment period.

With that, let us turn it over to our Chair Frank Pasquale.

Opening Remarks

Frank Pasquale: Thanks so much, Rebecca. I should have said during my introduction that I am at Brooklyn Law School and I am coming to you from Brooklyn today.

And so today we are convening a number of experts and we could not have done it without just extraordinary support from the Full Committee and from staffers delegated to our Subcommittee on Privacy, Confidentiality and Security.

So, I first just wanted to thank all members of the subcommittee. I wanted to thank our Full Committee and the Chair Bill Stead for helping guide us in the Full Committee toward this inquiry through the year. It has been a very challenging year in terms of planning, and I think it is very good that we are at this point now.

And I also just wanted to say an enormous thanks first to Rachel Seeger for her really extraordinary efforts in terms of convening the experts that you see today and reaching out and ensuring that we have a really number of voices from a number of different fields in a truly interdisciplinary approach here.

And of course, to Rebecca and to Maya, Rebecca Hines, and Maya Bernstein, who have been with us through the whole process.

And just to introduce in terms of the structure of my opening remarks and of my overall – of the overall – I am getting a little bit of feedback. I do not know if everyone is muted. Just in terms of the structure of the overall approach today.

Essentially, one thing that we are going to be going through is that we have a lot of objectives for the meeting at the broadest level. Our objectives are first to understand current policies and practices involving data collection and use with respect to privacy and security during the COVID-19 public health emergency. That is our first objective on a very broad level to understand these policies and practices because when there is something of such epical and world historical change and impact as a pandemic of this nature, there are going to be definite impacts on policies and practices.

Second, we are trying to understand the challenges and potential areas of clarification in light of these practices, new and emerging technology developments and new and evolving policy directions. And that is an area where the diversity of governance both within the United States and internationally can be both a challenge and an opportunity, a way of understanding what has worked, what has failed, and how do we move beyond certain failures to what has ultimately worked.

Also, to identify best practices in areas where additional technical assistance or guidance may be useful. One of the things that is so helpful to our National Committee on Vital and Health Statistics in which I saw the Standards Subcommittee last month and which I have seen throughout my time on the committee is its openness to expert advice. And I think that this is a real great opportunity to serve as a transmission develops between the thinkers and doers in civil society and academia and industry that are really trying to increase our understanding and effectiveness in combatting the pandemic and to those who are making decisions in Congress, in the Executive Branch, at state and local levels.

And at last just say before getting into some more meat of the issues that are raised today because they are very immediate issues and very important issues here that to give some history here, in 2015, NCVHS published a booklet on data use in communities. And we are building on that great foundation.

We are also building on the foundation of past PCS work on health care data beyond HIPAA and NCVHS work on this in terms of looking at the new data landscape because we would be remiss if we only thought of health data as being something called HIPAA covered entities. We ultimately have to think about this from a much wider perspective given the impact, for example, of big data on the ability of almost anyone who holds it to make health inferences, some of which are quite sensitive.

Now, to go a little bit further into some of the questions that were raised today and then to just give you a sense of why the subcommittee thought these questions were so important. In terms of what is the proper scope of data collection analysis and sharing in an emergency, there are two priorities or at least three priorities indeed that are in somewhat tension here when you think about the role of privacy, confidentiality, and security in the midst of a public health emergency.

The classic concern – you are getting some academic literature by word of mouth is that rules regarding the collection analysis use and sharing of data stand in the way of effective responses. There is concern that there are too many rules, too much bureaucratic control over data collection and sharing.

But on equal and opposite approach and sort of the response to that would say that we are gravely concerned that if we do not have very strong, robust, enforceable privacy, confidentiality, and security protections that we lose the trust in the system that is necessary in order to have overall effective response both right now and over time.

And then a final concern that sometimes is raised against those two tensions is that privacy, confidentiality, and security claims could be raised opportunistically to avoid the types of information sharing. We have also seen that of course in the realm of trade security, intellectual property, et cetera, some of the things that data blocking concerns raise as well – information blocking.

Trying to balance these types of concerns is something of great importance as we consider the collection, use, and analysis of data in the public health emergency. The deregulatory impulse towards saying that excessive rules or harming preparedness and the regulatory impulse to say that in order to build societal trust in trust in public health surveillance infrastructure, we have to have assurance that among all individuals that their data will be protected and used for the purpose for which it is being collected and not just sort of dissolving the ether or going to all sorts of inappropriate or unexpected uses.

Next among our questions is what are fair information principles for a pandemic? And, again, this tension recurs. We both realize in the midst of a pandemic that having data quickly and effectively is of utmost importance. We have seen that in some countries, they were able to very quickly get a handle on clusters to understand exactly where outbreaks were occurring. But they have been able to keep death to an extraordinarily low

rate. And just for some background here and I think that this level of – this kind of background is particularly important when you think about proportionality if we think about a country like Taiwan with about 28 million people. They have had seven deaths from COVID so for in 2020. The State of Florida with 28 million has had over 12,000. If you compare seven versus 12,000, there is much to learn and there is much to learn, I think, in terms of trying to have an infrastructure of data collection and understanding that would support things overall.

However, we also have to realize that the data collected here with respect to COVID is exceptionally sensitive data. As we have been learning throughout 2020, COVID is not a binary outcome with respect to say people just simply get better or have mortality. There are many perhaps lingering effects that we are learning about now and that means that this is sensitive, but also incredibly important data. When we think about fair information principles for a pandemic, we need to realize this balance between the importance of the data needs to be collection, but also the extreme sensitivity of some of this data.

Our next question is on what are best practices for properly cabining emergency authorities that supersede extra data protections? And I think this is an area of great importance. I will get into a little bit more detail later in my opening remarks. And I think that it is something that we have to think deeply about is as we respond to public health emergencies, do we think of the emergency as something that each emergency has to be responded to anew or are there generalizable principles of emergency response that would help us to better allow for data liquidity and access in the moment, but also would say attached to that data or to entities holding such data extra responsibilities to ensure that it is not misused over timed or even in the moment?

What data should organizations be collecting? One of the things that comes up as a tension within both health care providers and for public health agencies and others is one wants to be as comprehensive as possible in order to understand all dimensions of the crisis. But we do not want to overwhelm already hard hit and overworked professionals. In thinking about the types of data that need to be collected, the comprehensiveness of data, other issues here, we have to again have a balance in mind, a balance in mind both being able to have as much data as is needed in order to have an effective response, but not to overwhelm those.

And of course, this is something that I hear and read about quite often is a feeling of either disillusionment or just feeling overwhelmed by many data collection imperatives, some of which are unfunded upon health care providers and professionals.

Another issue is what rules are all right to override to advance public health and what should remain in force. And this gets to the point of both federal and state level exemptions, exemptions that have been issued with respect to HIPAA and with respect to state privacy laws by state authorities.

And one of the questions that comes up here is when are these exemption overrides and declarations of emergency appropriate. Some even question legality of some of them in terms of how far can they go, how are they best limited either in time or with respect to additional obligations for those taking advantage of them. These are really important issues as well.

Another issue that is closely related to this is what data rights may be contracted away and what should remain inalienable. When we think about this type of issue of contracting away, sometimes under a consent regime, that is, that you can consent to nearly any sort of use of one's data later on downstream in many areas of the economy. This is the classic concern about overreach in terms of service. But in health care, we have tended to be more careful with respect to the spread of data and its collection. Therefore, we have, I believe, a real responsibility as members of the Federal Advisory Committee looking into these issues to think about to what extent do we want to see new forms of private ordering. Where would we like to look into those new forms of private ordering and to what extent are these forms of private ordering inappropriate?

When we think about levels of identification of data, that is another issue that will be sort of coming through today in terms of when is there a need for identifiable data and when it aggregates data more appropriately. This has been a longstanding concern of experts in vital and health statistics. The need both to protect privacy of those in large data sets by taking away certain identifiers, but also the counter concern that if you take away too many forms of information from a data set that the data set becomes less usable. This is the classic tension between privacy and utility in data sets that we so often hear about in the privacy law and policy.

And so therefore, there is a concern about exactly what levels of de-identification are necessary and of course in the midst of

emergency, to what extent are these forms practicable. And this idea of practicability is one of great import today.

Moreover, how do standards differ at the local, state, and federal levels? Where is there a need for harmonization and where is there appropriate diversity of approaches? Going back to HIPAA's passage in 1996, we can see that as it was intended as a floor and not a ceiling for protection. It is not preempt. More stringent state protections with respect to health data.

And looking with respect to overall diversity, we both see a landscape in which there is some concern among data holders and others that there is a bit – that there might be too many standards that they need to pay attention, but also a concern on the other side that says that these are of great help in our laboratories of democracy and sort of being able to try and to look at the results of different approaches.

Now, thinking back to our NCVHS toolkit for communities using health data from 2015, one of the issues that we also hope to hear addressed today is once collected, where may data be disclosed and for what other purposes if any should it be used.

In thinking – one of the ideas that is critical to the future of a learning health care system as the Institute of Medicine deemed it back in 2007 was thinking really clearly about how do we improve over time and how can data that might be collected for one purpose also help with quality improvements and other purposes. And this is of grave concern in many areas within health law and particularly with respect to amidst in an emergency.

As we hear from both commenters and from those testifying at the hearing today, some of the things that may be in the future in terms of working with this might include updating our extant toolkit because in terms of that toolkit as a form of guidance and information, it is something that I think ideally would be added to in light of our experience in the midst of this pandemic.

Also, thoughts about data use agreements. How are data use agreements crafted? What are the best practices in their crafting?

Popularization of subtle data protection principles may also be in the offing as well in terms of trying to make sure that people can understand in an accessible way how information sharing occurs in the midst of pandemics and also in the midst

of public health emergencies in general because one thing I should also say as a matter of background for today's hearing is that public health emergencies are surprisingly common. After a hurricane, for example, there may be an emergency declaration with respect to data and privacy rules. Even if we are lucky enough to avoid something as epical and disruptive as COVID-19 again, we still need to think deeply about public health emergencies in general.

One of the other issues that really is, I think, unique and important about how NCVHS and the Privacy, Confidentiality, and Security Subcommittee can contribute to the debate is by providing an overarching framework and view of both covered and non-covered entities.

One of the things that we have seen throughout conversations about exposure notification and contact tracing apps in the conversation about COVID-19 pandemic response is certain volunteerism by very large tech platforms to get involved and to help local public health authorities, others to be notified and to understand the scope of the pandemic on the ground.

And we saw a very early example of this type of public spiritedness and interest in this cooperation between technology firms and those more traditionally health career-oriented firms with Google food trends. We are seeing it more recently with respect to the debate over decentralized versus centralized exposure notification and contact tracing apps.

And we can see it also with respect to the potential for data to be inferred about COVID-19 status by Internet searches, location, other forms of data, which are outside of the covered entities or entities covered by HIPAA.

In thinking through the use of that type of data both by private medical researchers, public health authorities, others, I think there is a role for ethical reflection and debate over the proper scope and extent of this expanding sphere of health data.

A lot of this is about health data stewardship ultimately. It is the responsibility for ensuring the appropriate use of personal health data. And we have to realize that failure to use good stewardship practices could harm individuals or communities, limit participation, and impede the use of data. Different types of data trigger different approaches to stewardship and the burdens of stewardship and the balancing interest can change from one type of data to another. This is something that involves accountability, openness, transparency, and choice.

I think the one thing that is coming through in terms of comments and in terms of the work that I certainly have studied for preparing for today in our subcommittee has looked at is community and individual engagement participation, the quality and integrity of data, ensuring security of data, all of those being really critical.

And also, one of the things we will be addressing or some of our panelists will be addressing is purpose specification, the idea that data should be collected for a specific purpose.

In thinking through these questions of data quality and integrity of potential de-identification of ethical tensions, I think we have so much to learn from today's panelists. We convene experts and public health, social science, law, data protection and other fields in order to address the collection analysis and use of data in public health emergencies. And as we do so, we realize this inquiry has several dimensions, both temporal and sector.

The immediate need is to clarify current information needs and opportunities to reduce the scope and severity of the current crisis. The long-term need is to develop systems of public health surveillance and responsive infrastructure that ensure that the US is never again in the tragic downward spiral that we now suffer from, which is a steady spread of a deadly virus, immense economic damage, which in turn reduces the real resources we have to fight the pandemic.

We must also understand the demographics of COVID to see the full extent of the disparities that both reveals and exacerbates. Racial and ethnic minorities, the aged, the elderly and other minoritized and vulnerable populations have been hit particularly hard by the pandemic. And given the risk of potential discrimination for all such groups, both the need for good information and the need to keep it secure is critical.

Sectorally we address both HIPAA covered entities and health data beyond HIPAA because there has been sustained interest in recruiting non-HIPAA covered entities to participate in programs like contact tracing and exposure modification.

Among HIPAA covered entities, serious concerns have emerged regarding new demands for data and lack of access to critical data. For example, it was recently reported in one state that coronavirus cases were spiking among school-aged children while the state was ordering counties to keep data hidden. There are problematic examples of privacy opportunism were exaggerated or

just plain false claims about HIPAA and related health privacy laws are simply deployed to rationalize stonewall. This is tragic on many dimensions both complicating pandemic response eroding support for vital privacy rules.

In an optimal scenario, the COVID crisis would spark unprecedented national levels of cooperation to maximize the use of helpful health data to slow and eventually stop the spread of the pandemic. We have seen this type of strong state capacity and social cooperation in many places, including South Korea, Taiwan, Senegal, Vietnam, Iceland, and Thailand. There is much to learn from all these jurisdictions. Indeed, there is much to learn for ones closer by. For example, David (indiscernible) has said of Canada that the US had equaled Canada's COVID mortality performance. At least 120,000 American lives would have been saved as of early September 2020.

My question there is what role did health data strategy play in all those jurisdictions? Was public confidence in data collection and use worth dissemination to health care institutions and providers important? Was this public confidence in data privacy, security, confidentiality, and utility more a matter of rules and procedures, investment of public health capacity, or something else?

As I conclude my opening remarks today, what I would say is that our ultimate goal here is to ensure that we can as a subcommittee advising a Full Federal Advisory Committee balance many different types of goals, values, opportunities in our ultimate recommendations with respect to the use of data in public health emergencies.

We are going to – we really want to hear from many sides in the conversation here. We have many experts from many different fields who are able to contribute to that. And I really look forward to the panels today. I will be moderating the first one. Two members of the subcommittee. Melissa Goldstein will be moderating the second. Denise Love will be moderating the third. And then we will have a conversation at the end of day, consider the learnings of the day, and to think about next steps.

With that, thank you very much and I will turn it back over to Rebecca.

Rebecca Hines: Thanks, Frank. I just wanted to note. We have one more member with us, who you actually just mentioned. Good morning, Denise Love. Do you want to read yourself into the roll call record?

Denise Love: I do. Thank you. This is Denise Love, a public health data consultant. I am a member of the Full Committee, a member of the Standards Subcommittee, a member of the Privacy Subcommittee. No conflicts.

Rebecca Hines: Very good. I believe that now is everyone. Frank, I will turn it back to you to – the panels.

Panel I – Data Collection and Use

Frank Pasquale: Thanks so much. Yes. And so I will be doing a very brief introduction of our first panel because we have all the full bios online for all of our illustrious presenters, who have done very interesting work in matters of public health, data security, data confidentiality.

We have on our first panel first Askan Saltoni, who is an independent researcher and technologist, specializing in privacy, security, and technology policy. We next have Allison Arwady, commissioner of the Chicago Department of Public Health. And we will have Robert Grossman, co-chief of the Section of Computational Biomedicine and Biomedical Data Science at the Department of Medicine and Chief Research Informatics Officer at the Biological Sciences Division at the University of Chicago.

With that, our first speaker – Ashkan, if you might be able to join. Thanks so much for joining us today.

Ashkan Soltani: Good morning. Can you guys hear me okay?

Frank Pasquale: Yes, thank you.

Ashkan Soltani. Great. Great. Thanks for having me. I really appreciate you guys having me here. It is a little early from California, but good to see you.

I want to kind of flashback in this discussion to say February or March. Folks, recall, as we were first encountering widespread news of the pandemic, there was an effort to essentially use data and technology to really inform our response. And with that, we saw a number of different apps and tools, emerge so we had, as we said, Singapore and South Korea had developed their own state apps for doing things like contact tracing. There was also a variety of technology, kind of platforms and tools to look at migration folks moving. And I want to kind of talk a little bit about that.

If we look back, we have a variety of responses from – ranging from symptom trackers. These were things like self-reported symptoms and access to tests and both aggregate and individualized data about people's health conditions.

We had essentially tools to do quarantine detection and enforcement. In China and other places, they came up with essentially immunity passports or ways for people to traverse borders.

We had tools to do contact tracing and this is the traditional, being able to tell who you have been in contact with, who an infected person has been in contact with such that health agencies can both monitor a spread of a virus as well as identify and have folks self-quarantine for those that might be infected.

And then we had this slightly evolved term which is exposure notification, which was a subset of contact tracing, which is to allow users to – or allow folks to know whether they might have been in contact and then decide what they want to do in those spots.

And as we discussed these kinds of topics, I wanted to point out that the data came from a variety of sources. Some of them were self-disclosed. Some of them were in partnership with health agencies or health labs. Some of them wore smart thermometers, tools that consumers would buy, which would act as proxies. We have things like even the use of Ad Tech data so data from what is known as bitstream data of the use of mobile apps and other sources being used to, for example, identify when people migrated from one state to another or people were congregating in mass in one location. We had basically a rush of tech that kind of – to address or respond to the pandemic partially because of lack of any concentrated or coordinated effort at least here in the US, and partially because of just tech wanting to step in and provide tools.

But as Frank said earlier, a lot of these responses were outside of covered health agencies, covering health entities, and outside of the typical health protections that we see. And a lot of it was done completely by the platforms.

One area that I want to focus on is the use of this technology for what folks would argue is one of the critical features and dealing with the pandemic, which is this idea of contact tracing and exposure notification.

As I said, Singapore and South Korea had developed apps that were somewhat successful. Australia and the UK were also building some apps. These were based on a model where the app would use location information so location about where you have been as well as information from your Bluetooth device, from your Bluetooth antenna to identify whether you are in proximity to someone else based on their Bluetooth signals. And the apps at least in Singapore and Korea would require that the user identify themselves by name or by government ID when they first set up the app and then those apps would then report to a central health agency who an individual had been in contact with such that the health agency could determine whether they were in contact with someone that had been infected.

Those tools and those techniques have very much some privacy concerns if you are revealing your whereabouts 24/7 as well as who you have been in contact with to a health agency or even a government entity. I think a lot of folks might have some concern for privacy as well as some concern with even adopting or volunteering adopting –

And in response, the tech platforms stepped in and came up with a kind of their own architecture or solution to deal with this in a more privacy-preserving way. And this was initially the Google app contact tracing API. This was a toolkit or a framework that Google and Apple presented or promoted an issue called the contact tracing API and then later called the exposure notification API that attempted to do the same type of function, essentially identify whether a person has been in contact with someone else that was infected with the disease, but do it in a privacy preserving way in a distributed and de-anonymized way. And they did so kind of I think unilaterally.

Part of a thing to also remember is at this time, they were in the process of simultaneously building this technology, but also as the gatekeepers for the two dominant platforms, they were also responsible for approving all the other apps that Singapore and South Korea and the UK government wanted to build, including those that would collect location of Bluetooth in the background.

There was also the second issue, which is a small issue, but worth noting that at that time, there were some technical limitations on the way these apps work. The platforms Apple iOS and Google Android limit how well apps can collect things like Bluetooth information in the background. And in fact, the Singapore app and the South Korea have limitations where they were not actually detecting exposure events or contacts and were

kind of pressuring the platforms to fix this part of their operating system as well. There was increased pressure on the platforms to do something both from a pragmatic perspective as well as from trying to step into their role as gatekeepers. They came up with this Google Apple exposure notification API, which is just briefly is a toolkit that does much of what we say that is necessary for exposure notification or contact tracing, but it does so in a distributed way.

And the way just briefly, I am sure everyone knows this by now, but I will just go over it briefly. If I opted to use one of these apps and tools and now the tools are built into one of the platforms, iOS built in my default now. If you enable it, you can immediately start participating.

My phone, for example, sends out these synonymous identifiers that would essentially just notify people in my proximity of my identified information although it is rolling an anonymous in some sense. And if Frank and I are in the same room, Frank would get one of these notifications and his phone would record these encounters on his device without revealing it to any other authority.

And then at some point I was tested and tested positive with COVID, had I installed one of these apps, I would be able to notify essentially the system that I was exposed and then the system would then pass on my proximity to Frank and Frank's phone would then match – look up and see whether he was in contact with me and then it would match and generate an alert on his phone. No central authority would necessarily be notified of our encounter. No additional information per se would be revealed to anyone. And then Frank would have the option, the choice to then take some action, which is he could potentially contact the health agency and report that he was in contact. He could actually self-quarantine and take action. That is the more privacy-preserving API that has been proposed.

Briefly with my few minutes left, I want to just talk about some of the privacy considerations and then some of the other considerations with taking such an approach. First off, the approach, as I said, is for voluntary by Frank and I and not only voluntary in the sense of adopting the app, but were Frank to receive one of these notifications, he would have complete autonomy and choice of whether to respond and pay attention to these notifications. And for many reasons I will get into, that is itself a question. Will someone respond to a notification from one of these tools without having some additional

assurances, someone to talk to, someone to vet whether the results are real.

As we know, one of the core functions of contact tracing traditionally is someone to convince you to essentially restrict your freedoms, not go back to work, to not to take – to convince you that this is a serious thing that you should take serious. As we know in a current world where people are refusing medical advice to even wear masks, there is a question of whether a notification pop-up along with your email and snapchat – will actually cause people to take an action.

That aside, there are also real questions on whether a technology like this would work, whether it is Bluetooth based or location based or whether technology solution by itself is sufficient to provide a level of quality of service. As we know, there is a high risk of false positives. This is – Bluetooth and these types of signals or even location as proxies can yield matches when there are none. If Frank and I were wearing personal protective equipment or we were in the same location but separated by a wall or by a floor, we might alert as being in proximity with one another when in fact we were not.

There are also issues of kind of on the other side of false negatives or over confidence. These systems do not actually work until a wide number of people use them. In fact, we have something like 81 percent smartphone penetration in the US. Even if 100 percent of the current smartphone population installs these apps, we would get at best case, 64 percent kind of detection rate using these technologies and much, much less in the early days. So separate from false positives, we have this issue of false negatives where people will potentially rely on this technology as a false sense of confidence that it is safe to go out when in fact they might have community spread or widespread outbreaks in their area without knowing it.

Separate from the efficacy concerns, there is also the question of whether the privacy concerns in these technologies actually are sufficient. As I said, there are platforms – a very good job, making sure that there is no central authority that can necessarily monitor one’s actions or one’s kind of contacts. But the architecture or platform actually yields itself to other types of attacks where other dedicated attackers might be able to correlate some of these proximity beacons and some of – you are basically identifying information. And this could be simply by setting up one of these Bluetooth detectors in conjunction with a camera or some closed-captioned video footage, which would correlate when peoples are meeting these beacons and some

other form of identification. There are additional privacy concerns as well.

And then lastly, an area that I am particularly most concerned about and I think is important to touch on is that the decisions to make these systems distributed and to make these systems for privacy preserving, actually then indicate a number of security concerns that are present in this type of architecture. Specifically, as I said, no central authority will know whether that there are outbreaks or notifications. When Frank receives that match on his sofa that he and I have the contact, if he takes no action, no one else will actually be aware of that.

And one of the challenges is that given that distributed nature of the protocol and given the architecture, there are a number of attacks of abuse. There are ways to do what are known as denial of service attacks by shutting down the network or flooding the network such that again even if we had 80 percent coverage that the signals would not actually get through to the network.

More importantly, one area that I have been working on recently is showing that there are actually ways to generate false alerts. Again, there are techniques that you can use to take my signal and essentially in real time, rebroadcast it via a computer or via – configure a device that is not a cell phone, to all of your devices such that even though we are speaking remotely, if I had some malware or if I had some essentially one of these sensor networks set up, I could be broadcasting my beacons to all your phones and then the moment I then disclose myself as being infected, all of your phones even though we were not in contact, would light up that you might have been in contact.

And while that might seem like a far-fetched attack or a far-fetched consideration, there are ways to do that in a targeted way say around an election to generate notifications and essentially this information around election to at least cause panic and have people question whether they go to the polling booths or they go out into public.

And, again, this is an attribute of the decisions of the architecture that was made to do this in a more secure, sorry, in a more privacy preserving way and protection less securely and those were the tradeoffs.

Kind of coming back kind of zooming out of just the exposure notification API, although that seems to be the way everyone is going, my primary concern with some of these technological approaches is that they are being done essentially unilaterally by large tech platforms that pretty much dominate the distribution channel for these apps and therefore have decided or made decisions about where those right tradeoffs are with regards to both privacy and security and efficacy, independent of any kind of policy leadership around these issues.

And while the health agencies and administration and others, at least in the US, are catching up, there is really a gap that has been filled by these platforms and widespread adoption based on these tools. And I think we will have only a couple of bites or even one bite of the apple. I do not think we will be able to convince people to widely use other tools should these get adoption as we see many states rolling out, and it is possible that not only are the tools insufficient from an efficacy perspective, but are in fact create new vulnerabilities and opportunities for abuse that I think would at the very least cause people to not want to adopt these tools and worst case cause actual panic and concern. That is kind of the lends that I am looking at things through. I would love to take comments.

Frank Pasquale: Thanks so much. That was a really clarifying and illuminating presentation and I look forward to the discussion afterwards.

Our next speaker is Allison Arwady. Is Allison on?

Allison Arwady: I am.

Frank Pasquale: Oh, yes. Thank you. Great.

Allison Arwady: Good morning and thanks so much for having for this important conversation. As the commissioner at the Chicago Department of Public Health, my agency has the responsibility for really turning all of this data into action. It is my team that at the end of the day is reaching out and calling cases and contacts. Every week we are looking at our local data and making decisions about where to push testing resources, where to do additional outreach, how do we need to connect people. And certainly, I think, COVID has pushed a lot of these data privacy conversations very much into the public mainstream discussion in a way that I think is going to be very healthy in the long-term because certainly at the health department and particularly at the local level, we have been having a conversation for years about these issues. Without identifiable data broadly, we would

not be able to make a lot of the progress that we have been able to make around issues like HIV, lead poisoning prevention, any of the 70 communicable diseases that are reportable to us by law.

But I think there are two things that I want to highlight. One is that the public health department at the local level very often is playing a system data coordination role because of data silos that have developed over decades and frankly in the absence of a national health care system.

One of the things that also really differentiates us from Taiwan, for example, as was brought up initially, is that in most other countries in the world where people are seeking health care across the health enterprise, you are better able to have visibility into where someone got a test even if it was in a hospital or a clinic different from my own.

You are able to understand what someone's course of care has been, what their underlying conditions are. You have information about their demographic information, all information that is here. The way that we have data broadly set up in the US public health department ends up very often playing a role of needing to pull together both public health data silos and frankly our health care silos.

The other piece is that – to the point of the last speaker. Technology has been outpacing the public health practice and frankly a lot of the rules I think that we have in place at the moment. We are really excited by a lot of these technology advancements. Very often that has been our rate-limiting stuff. And I think that this pandemic in very good ways has brought attention to a lot of the outmoded public health data systems that we had. It has required us to work to try to modernize our public health system just in three to six months. It is an amazing opportunity. It is one that we are very much right in the middle of here in Chicago with many of our health care partners in conversation with the state, in conversation at the national level. But that is even just the basics of the data reporting and I think how these additional technologies are going to plug into this is such an important piece.

Broadly, I think state and federal law have not kept up with public health practice in this space. And I want to just highlight that at the local level, the Chicago Department of Public Health – we baked privacy and security into everything that we do every day.

Just to give you a quick sense of that. Any project that has a data security implication is going through our information security office review. Any contract that has a privacy component is being reviewed not just by contract attorneys but are privacy attorneys. Any partners, research projects that would involve individual-level data sharing would go through an institutional review board. And where there is IRB approval, we typically do require a data use agreement any way. And I would be happy to talk some more about that.

It is really important that our privacy compliance program, we have got policies, procedures, annual staff trainings, privacy complaint investigation process, et cetera. We have counseled well versed in privacy in the public health context because as you know, HIPAA is a not a synonym for privacy, but it is often used that way.

Our legal council here has to think a lot about the privacy and confidentiality restrictions that go way beyond HIPAA. We have dozens of acts around communicable disease, sexually transmitted diseases, our lead code, our substance use and mental health privacy acts, WIC rules, the federal privacy act, et cetera. There is a patchwork of privacy rules that mean some data can be used for some purpose. Some cannot. And this is complicated at best and I think can make it hard for the general public to understand how we protect the rights of the individual, but also facilitate this crucial public health work.

We want to make sure we do not just like land on the default answer of no when it comes to data sharing, but we do want to err on the side of caution there.

And then in addition to the legal question, can we share data, there is this really important public health ethics question, should we share data. Here at the local level just to give you a sense, we have a local public health ethics committee that looks at proposals. We have also pulled together a data governance committee, which particularly in the time of COVID where we have had more data sharing, for example, among hospitals, we have pulled together a committee with experts from all of those data sharing partners to really make decisions with us about how that data should be governed, how it should be shared, how as we work together to break down some of these silos that allow us to have an appropriate response. We continue to protect the individual privacy rights that are so important.

I think it is important that we place this conversation about COVID and emergencies in the larger context of public health

laws. You look at HIV just as one example. Twenty years ago, there were such strict privacy rules around HIV data that even at the clinical and public health where we want to use data for action, we were often stymied from doing that.

I think as we have worked to make sure within the appropriate privacy protections, we are able to use that data for action. For example, we now have technology in place where if people with HIV have fallen out of care, they are not – it has been a certain amount of time since they have seen a provider. They have gotten their viral load checked. We are able to know that on a registry level and then in a way that does not compromise privacy. If one of these individuals comes into an emergency department in Chicago, there can be a flag on that person's chart that basically says this is someone who may be out of care. Here are the things that we need to do to pull them back in.

Similarly, around lead poisoning prevention. As we have been able to think about predictive models, I think some of the most important role that public health can be playing here. Of course, our goal is to prevent disease, not just respond to it. And I think predictive models around things like lead poisoning where we have been able to, again, for example, where a child is being seen in an individual provider's office, we are able to at an individual level, what is the address of that child who has not been lead poisoning. Use tech to link that up to our data at the city level and say is this an address that would be at increased risk for lead poisoning. Does this child have other risk factors that would say we want to do something preventive? We are able to then ping back to that provider in the visit. This is a child who we want to do a proactive lead inspection on. This is a child who we want to make sure is getting tested earlier.

These tried and true ways of using individual data for protecting the individual, but also for the public good I think are the place to start and learn from in emergencies. Privacy certainly has a nuance in the context of public health. The Illinois Constitution has an expressed right to privacy. The US Constitution has an implied right to privacy. But as you know, that right is not absolute. The heart of public health is this push and pull of rights of the individual, rights of the public good. It is the distinguishing factor between health care where the emphasis is on the autonomy of the patient and public health where the focus is on the public good.

We have long recognized there are spaces where the greater good can outweigh the rights of the individual. We have mandatory reporting laws for communicable diseases, child abuse, and neglect, blood levels, et cetera. These are constitutional at some level. They do infringe upon the privacy rights of the individual.

And so, I think COVID at the end of the day has been a real opportunity for us at the local level to make data as transparent as we can for Chicago while protecting the individual level of it. But it also I think raised the need to perhaps modernize and make sure that the appropriate amount of data is available at the appropriate level.

Local health departments are aware at the end of the day. We are typically making those individual-level interventions and working with individual providers and it is very important that we are able to continue to use that data for the public good.

Thank you very much and I look forward to the conversation.

Frank Pasquale: Thanks so much. It was really helpful to get that level of detail and to hear about the ways in which your department of public health is exemplifying some best practices with respect to the type of difficult balances that we have been discussing earlier. I think there is a lot for the discussions now. Thank you.

I see that Robert Grossman is on so I will turn to our third panelist. Is that good, Robert?

Robert Grossman: Yes, that is good. Thank you very much. Thank you very much for the invitation. I am going to talk a little bit about data access in a public health emergency from a slightly different perspective.

The starting point for this – I was one of a number of experts involved in the Rockefeller Foundation Report, advocating for a national COVID-19 testing and tracing action plan. That report is still valid. It called for testing to 30 million per week. The second recommendation was to launch a COVID Community Healthcare Corps for testing and contact tracing.

And I think the third is my particular interest and what I want to talk a little bit about today is we are doing a lot of testing. There is a lot of discussion about testing. But oftentimes, I do not think we are making maximum use of that testing data. Certainly, there are challenges balancing security

and privacy with sort of doing interesting things with that. But part of it is we do not have appropriate platforms for working with data that is collected during a public health emergency and getting the most utility of that data while balancing privacy and security and that is what I want to talk about. I am going to talk about the general question of how do we do this.

I am going to – when we look at this, there is quite a bit of data out there and I think one of the things we should be thankful for the community for is a lot of non-traditional groups and non-traditional organizations have formed. There has been a lot of safe data sharing. Just to remind people, the reason we have the progress today of vaccines and potential drugs is because the original viral sequence for the COVID-19 virus was shared widely. It did not have to be shared, but it was shared widely very early.

As COVID and other health emergencies that are of high-risk base appear, the viruses mutate and so there are various projects that maintain virus sequence data. There is a lot of incidence in tracking data. They are noteworthy of particular private projects like the COVID Tracking Project. The work from Johns Hopkins, the New York Times, and others in addition to CDC and the public health authorities.

There is clinical data being collected by a number of NIH agencies. This includes the N3C Consortium, the BioData Catalyst program from NHLBI, NHGRI sequence data, a new project for imaging data from NIBIB. There is a variety of clinical and imaging data. And for those of you involved in the building of modeling, trying to understand what is going on on the spread. You know mobility and behavior data from sources from Google to some of the other networks are absolutely essential.

This is a busy slide, but it is often – it is certainly the case that we have to think of HIPAA and we think of limited data and de-identified data under those regulations and related regulations.

I take this view as trying from nontraditional sources to get data. What are the knobs we have to make that data available to improve health outcomes, to get people back to work earlier, et cetera? We have a lot of knobs.

In addition to removing information so that data is less likely to cause harm or aggregating or a times disaggregating data. For example, in the first talk, we heard about data collected for contact tracing. In that protocol, the trajectories are not long

lived. They are restarted, if I remember correctly, every ten minutes. And there are lots of ways to take data that could be more of a potential harm to privacy if it were a continuous tracking safe location and just having location reported maybe once a day. Obviously, if it is reported from home, there is still a problem, but it is a different type of problem and you can make the provider aware of that.

In addition, we can support different types of analyses. We can sort of have all digit queries that go on siloed data, as we heard about in the last talk. The data could be made available to different groups and consortiums and community and public under different types of agreements, including both traditional data use agreements, data contributed agreements when they apply as well as lighter weight data with less service.

And importantly, these large tech providers that were mentioned in the first talk are giving us tools that we have never had before in public health emergencies at the scale we have them now for analysis of data. Amazon, Google, IBM, Microsoft. They all have very capable cloud-based platforms that come with services that make it easier to provide security and privacy, easier to analyze data, easier to build predictive models using machine learning as the type of predictive models we heard about in the last talk. All these things can come together. There are a lot of knobs and I think it is – as you will see in the next few slides, it is interesting to ask how can we use these knobs to balance what need to do in a public health emergency with protect and security and privacy.

I like to think of this in silos. Often with – clearly, with a public health emergency, the first silo involving testing, contact tracing, quarantine, and all the other activities that take place are absolutely essential. When people get sick, the patient care and hospital operations that are part of covered entities involve not just taking care of patients, but making sure the supply chain, the surge capacity, quality improvement are all in place. The Institute of Medicine Learning Health System was described in this about quality improvement and quality improvement, as we learn more about COVID and other public health emergencies is critical.

Then there is the research governed with IRBs, data use agreements, data contributor agreements. But I would also like to talk about two other things that are very important. One is do the decision makers making decisions about communities at the local, state, and regional level – do they have the information they need? Oftentimes these are incident levels, incident

trends, hospital capacity, supply chain, et cetera. And importantly, does the community have what they need to make decisions about what they are going to do each day, where are the hot spots, how can – what you might think of as a hot vector in closed restaurants, bars versus outside restaurants, well separated, et cetera. How can they get the information?

I am going to talk a little bit about the data platform to support these other three silos. I think of this as sort of complementary to the first two silos that I think most of this will be part of. I would argue that in a public health emergency, it is really about leveraging data any way we can get it and respecting security and privacy as we do that.

I am going to talk about a particular technology that has been used for the last five or six years, but I think is appropriate to consider for public health emergencies called data commons. The idea of a commons is a very old idea. It goes back in law to something as simple as a pasture in a village where if it is used by the community and managed for collective benefit and there is enough grazing land available for the entire village. But it is not used responsibly, one individual's cows can reduce that. The same for other things like fish, et cetera, which can be depleted. Commons are held in common, not owned privately, but a group or a community can manage for individual collective benefit. It is an extremely powerful concept.

Data commons are much more recent, leveraging sort of the large-scale technology provided by some of the tech giants. They combine data, computing infrastructure. But the tools, services, privacy, and security guidelines so that data can be shared with the community while protecting privacy for the benefit of those that contribute it.

Importantly, NIH has been building these for the last four or five years. The Genomic Data Commons from the National Cancer Institute – I have been a bit involved in. It serves – there are over 100,000 users each year of that data. It is the largest repository of cancer genomics data. It is used around the world. It creates a resource that benefits the cancer community that is trying to improve outcomes for cancer patients. And there are more recent versions of this for cardiovascular disease, which is by NHLBI, which is so important for this particular emergency.

Traditionally, we think of how we can protect the subjects when data is collected. But the flipside of that is everyone has the

right to the benefit of good health and benefit from research. And I think Commons are about balancing these two.

If you look at this very broadly and I think it is important, we know about databases for projects, warehouses for organizing data for organization. Commons do it for community and in this context can support medical, scientific, and health care data for research as well as data to support decision making in a public health emergency while providing security and protecting privacy.

I am going to talk about a particular project a number of us have been working on called the Pandemic Response Commons. It was started in late March. It is nascent activity. I will talk a little bit about the long-term purpose, but it is a Commons infrastructure for a pandemic and epidemics. It is designed so different groups, different communities, state and local and regional can set up their Commons.

We have done this in the Chicago region. It is open source software so anyone can do it. There are legal templates. For example, templated data contributor's agreement, data use agreements design to be used with IRBs. There are a number of different data types supported and the agreements are out there so it is designed so that there is both the software, the legal infrastructure that could be used for a particular instance of this as well as the principles by which this operates.

This is one focused in Chicago in Illinois. We have put in place for clinical and subject-level data agreements with RUSH, UIC, University of Chicago, NorthShore, Sinai, Saint Anthony, and other organizations in the Chicago region. We are supported by philanthropy and in-kind donations with civic organizations such as Matter and P33 in Chicago. There is a neutral not-for-profit called the Open Commons Consortium that brings us together. Amazon and BioTeam and other private entities have provided extremely important in-kind contributions. Our focus is not only doing this for Chicago but allowing other regions to do this.

We have a number of different data types. We have a data model so the data is harmonized. People can explore the data. Most of the data is controlled access, but there is a lot of open access data that can be explored. The knobs that I showed in the other slide are available.

There is workspace for people who analyze data with modern tools such as Jupyter Notebooks and R-Studio.

There is a project that is beginning to collect viral sequence data in the Chicago region so that we can look for changes in the viruses that affect us in a region.

And there is an app that allows someone at a particular point with no continuous tracking of their location to either voluntary their location or not but provide their health status as regular or green. Importantly and still, this could provide information about hotspots and we could put simple questions in here to begin to understand hot vectors.

I want to conclude with some recommendations from this project. As expected, it took a long time to get the agreements in place. We have statistical summary report data coming in right now. This is sort of count level data. It is importantly by – it includes accounts of various types of various communities by race and ethnicity, which is so important when there is disparate impact.

My first recommendation is set these up in public health emergencies and leverage them to complement public health, its standard hospital operations with communities and research could do.

My second is for when there are two commons that operate at a given level of security and compliance, for example, our commons file NIST 800-53 at moderate and interconnect following NIST 800-47, form trust relationships so different regions can share data. We can also federate queries in this way.

Importantly, it took quite a while to set this up even though it was a health emergency. So, set up a persistent infrastructure like this that is ready for future responses to epidemics and pandemics and have data sharing agreements that are in place and data infrastructure ready to go. We intend to do that with our Commons. If this is the new normal, that is going to be really important.

And finally, agencies, foundations, and others that fund research, fund data collection, fund data analysis should require that researchers share their data with some infrastructure like this.

That is my last slide. Thank you very much.

Frank Pasquale: Thank you so much and I really appreciate both the level of technical detail and the relatability of that

presentation because I think there is just a lot there for all of us to learn from.

I will now turn to the Q&A. We have until 11:30 for Q&A. I have some questions, but I do not want to be – you have already seen a lot of me so far this session this morning. I will just doublecheck with the participants to see if there are from our committee that wanted to have a question. Please do not be shy.

But I will start first with a question of the first presentation on Ashkan's, and then I have also questions for Allison and for Robert.

One of the things that I was very interested in your presentation, Ashkan. It was about the question of manipulation and hacks or other forms of untoward interference with these types of – these centralized apps. I am wondering. Have you seen – I saw a debate in Europe about the DP3T protocol and other protocols. Some said that if there is a more centralized approach then it is less susceptible to these sorts of untoward interference. I am wondering if first of all just in terms of your perspective, are there alternative architectures that would avoid some of the security concerns that you raised and secondly if you have any recommendations to the committee about efforts by reports by security experts or associations on the relative merits of centralized versus decentralized exposure notification contact tracing apps?

Ashkan Soltani: Absolutely. And as you know the DP3T were essentially one of the inspirations for the Google Apple notification API. I can send both – they have a security document, which outlines these types of risks. And the NHS UK cyber group, which I believe is related with GCHQ did an analysis of their location-based app early on and identified similar types of manipulation risks of those apps. And I can post a link in the chat as soon as we are done here with those or I will email those to you.

There are tradeoffs. Right? So, there are always tradeoffs. A centralized approach has kind of less privacy-preserving properties. And if you, for example, take control of a centralized system, you might have, in fact, more ability to wreak havoc, but you might secure that centralized platform more. The properties of the distributed system, particularly the privacy-preserving properties of the distributed system make it very difficult to mitigate these types of attacks without adding additional privacy invasive telemetry.

You could, for example, get aggregate statistics on – an example I gave where your phone would notify you because you were in contact with me. You could have your phone report aggregate statistics to the central database that will be distributing these notifications. I believe APHL is going to be doing that here. They could, for example, record telemetry about uptick in outbreak, which might help them, for example, mitigate these types of attacks, but might also help them know where there are hot pockets of outbreak, but that would go against the privacy-preserving properties proposed in the protocol. There are different approaches and they all have tradeoffs.

My issue I think in my talk is that the tradeoffs made in the Google Apple exposure notification API made them kind of unilaterally or bilaterally without I think the opinion of bodies like yourselves and perhaps not in the right balance with both the utility of the apps as well as the ability to mitigate these types of attacks.

Just to put a final quote on it. The need to secure the platforms falls on the health agencies implementing them. The API provides health agencies with the tool to essentially deploy a tool, but it is on the government health agencies to choose to deploy them to figure out how to secure these systems with the fact that they do not have any additional telemetry. It would be a very hard thing to do, I think, for a government health agency to do.

Frank Pasquale: Thanks so much. That is very helpful.

Before I get to my questions for the other panelists, I did see a question in the Q&A that I will put to all the panelists because I think it is a very thoughtful one with respect to consent. In the Q&A, the question is can you talk a bit about consent. It seems that one of the key aspects of using data under health exemptions is waving consent. But some of the silos of purpose that Dr. Grossman talked about are focused on research, seemed more in line with the standard research. It seems that the same information collected by public health authorities under exemption could be leveraged for research with consent. This suggested infrastructure for managing data as well as consent information.

So to just give a little bit I guess more background on that idea, I suppose one thing the question is getting at is is there more of a role for consent in situations where say it is after the emergency has passed when research may be done on the data. I will throw it open to all panelists.

Robert Grossman: Let me say something. I think one of the ways we looked at the data that was collected for the pandemic response comment is it became clear pretty early on that a lot of the impacts on the population are going to be long lasting and we are going to need information for a long time. We were very careful and there was a tradeoff because we were very careful to make sure that the data we got was consented sufficiently so that it could be used as standard research or there was explicit consent for like the progressive app for mobile and web in which that data could be used, but preserve privacy so that it could be used long-term as well as for – I did not go into it – for aggregated statistical data. It is at such a level that it can be used long-term.

I think that was one of our guiding principles, assuming that the other silos played in a different way. We are looking at this that this data has to be around for a while and sufficient consent has to be there so it could be used and can be intermingled and yet used best practices for protecting privacy and security. It certainly was a big part of how we thought through things.

Allison Arwady: I would maybe say on that that all of the data that we are receiving at the Chicago Department of Public Health we are using to sort of answer on a daily basis questions that are about collectively using that data. What our IRB is often most charged with determining is are these questions that we are working to answer in line with traditional public health practice or are they really getting into more research particularly something that may outlive or have more if you are needing to go back and do any additional interviewing, certainly sample collection or anything like that. But even if there is additional interviewing, we will then have much more in terms of the data use agreements and the real like why are we asking these questions, why are we doing this and require more individual level consent around that.

So just to make like a really concrete example where we are – say we have an outbreak like in a setting in Chicago. We are in there. We are interviewing the people. We are asking questions. We need to from a public health perspective, really understand what was driving that, what can we do to limit it. As soon as we make that a case control study where we are not just interviewing the people who got COVID, but perhaps the people at that gym or that restaurant or whatever setting it is, who did not get COVID, it then does actually start to have a little bit more of a research feel to it although it is still in lines of public health practice. In that setting, we actually will sort

of do a consent, an IRB, and say you have not been diagnosed with COVID, but we would like to interview you if you are willing for this purpose.

There is this like very immediate like every single week where are we going to dive in a little bit more than what would be typical. And then especially, I think, is this a question that actually needs some expertise and some resources that go beyond the Chicago Department of Public Health?

The other example I would give is that we have been very focused on racial and ethnic inequities from the beginning here at CDPH. And we have a race equity rapid response team that gets de-aggregated data that is at a neighborhood level and we use it to drive testing. But also, we really wanted where there was a lot of missing race and ethnicity data we wanted to use an imputation process to understand what is that likely to look like and we needed to partner with an academic institution to do that. So did a whole IRB around that. Did not do individual-level consent of people because there was not additional things that were asked or additional things that were needed and it was more driving our understanding at the public health response, but still all of – because it is individual level data, all of the requirements around the privacy and the security and how are you going to use this and how are you going to store it that we would have for within CDPH then need to extend to the academic institution. It is this line between using the data that we have.

If we are collecting additional data to answer a question that for us triggers – there needs to be some more level of individual consent certainly if you are collecting genomes or anything like that, but even just questions that triggers it. And then separately, are we pulling in some partner to help us with analysis, that also triggers an additional level of review. And in some cases, depending on what the goal is or whether there is any risk for identifiable level, that is when there will be some more. But this is where the data use agreements and some of those details really come into play and that is what our IRB and our ethics board, et cetera, are looking at really on a weekly basis.

Frank Pasquale: Thank you so much. It is a very comprehensive answer. It really helps us see the degree of care that has put into a lot of this data collection.

I see in our participants two hands up. I saw Denise Chrysler first and then Vickie Mays. Denise, if you would ask your question.

Denise Chrysler: Thanks a lot, Frank, and thank you to all the panelists. A lot of food for thought here. I have two questions. The first one is for Commissioner Arwady and I believe it may also be relevant to Dr. Grossman. When HIPAA came about, it was contemplated that we would have a national identifier, a patient identifier. And you had talked a lot about especially Commissioner Arwady, challenges in data being siloed and bringing data together from all these disparate places. Was this a matching issue or was it other types of issues? To what extent would funding of a national identifier, a national patient identifier assists with the silo of data, the data silo issues?

Allison Arwady: Yes. Thanks for the question. Certainly, the absence of a national identifier hinders us in this. But I would say it is more than just the national identifier. It is that any time you have an identifiable piece of information like an identifier or an address or whatever it is, it is more that there are a lot of strict requirements around who we are allowed to share that data with at any point.

Here is an example. It took a lot of work for us to be able to match up people who are in a housing choice voucher program with children who have lead poisoning. The sort of legal ability to sort of do some of that match where you are taking data that has been collected in one program particularly when there is a health aspect to it and match it to any of the other programmatic social indicator pull it together. Certainly, an identifier would 100 percent help with that and would help protect some of that privacy. But still the limits are often just that we are not – we are often precluded from sharing health information without some very specific additional carve outs or rules or findings at typically the state level around this.

A national identifier would help hugely. I think things like testing, things like vaccines that are coming up in the COVID response, anything that helps pull it together. But it alone would not solve the fact that we have a lot of requirements right now that keep us particularly at the local level from linking data in ways that would probably make us more able to respond.

Take one other example just to give you a sense of this. The prescription monitoring program for opioids where anybody who is

prescribing an opioid, it goes into the system. That data is not available to local health departments. It probably should be, but at least in Illinois, it is available at the state level, but not at the local. So where I have someone who has an opioid overdose, I have no way of linking that person to the person who perhaps prescribed an – I have no way of knowing that is the same individual who has gone through 12 different systems because we are right now still precluded from getting a lot of the information.

Long answer, but an identifier, anything that would help hold these together I think would be a step in the right direction, but it is not sufficient to overcome right now what are a lot of limitations in how we can connect data without doing a whole lot behind the scenes work because of privacy.

Robert Grossman: I want to build on that and just make another comment that is related, but slightly different. I think Dr. Arwady addressed sort of the broader issues. I just want to talk about perhaps a simple thing, HHS or some other community might do that could move us forward.

There is technology for privacy-preserving record linkage using cryptographic-based identifiers that change. And having something like that in which there could be ways that short-term identifiers could be used that preserve privacy in a sense that could not be easily inverted would allow certain types of record linkage with privacy. It would be quite helpful when data is distributed in different siloes.

I do not think there is a huge technical issue. There are policy issues because of liability versus technical tradeoffs. But there is partly IP issues, partly someone has to stand something up. Partly, it is the role of the government I would argue that could sort of agree upon the standard in the same way they agreed upon standards for hashing and other things they could do this. It is not a patient identifier, but it is a way to link data in different locations in privacy-preserving ways, which is as much a policy versus a technical issue.

Allison Arwady: Yes. And, Dr. Grossman, I would totally agree with that. I think where we have been able to solve this, it is getting the hashing done. It is getting the tech done and then getting the sort of legal pieces that surround that to accept that this is a reasonable way to do it. I think that is an excellent --

Robert Grossman: Plus, the liability, which is why I think the HSS can sort of be of help here potentially.

Frank Pasquale. Thank you.

Vickie Mays, if you could join in with your question.

Vickie Mays: Right. Thank you. Denise actually started part of my question. First, let me just thank the panelists for incredibly informative presentations in the short amount of time that you had.

But I want to go back to Commissioner Arwady and see if I can get just a bit more detail on a couple of things. Can you talk a little bit about how it is that you are able to set up a structure that would allow you doing an in-person visit to be able to connect data up? I was really impressed with that. And in a public health emergency, you would want to be able if someone is showing particular symptoms to be able to ping the physician during the visit. You talked about that. That would be useful if you could say more about that.

And second, I guess what I am impressed about is your ability to crossover many privacy, confidentiality, and security boundaries. I am trying to understand what in your infrastructure has resulted in your ability to do this so successfully.

Allison Arwady: Sure. Thanks. Two things. One is that each of these projects has taken a long time to get done and has been done very much with clinical partners and tech partners who have been able to help with some of these hashings like Dr. Grossman was saying. Some of these behind the scenes ways of making sure that we are not – always like privacy is – like we take so – every project we do sort of starts with privacy and like what are we doing to make sure that if we are going to do anything that moves any data beyond our ultra-protected within the health department, it has to have all of the pieces built around it legally, but then also from a technical standpoint.

This has been very much a partnership with people in Chicago who think about these issues, who want to help build the tech with the academic centers. And so just to give – like there have been a couple of examples and I just touched on two of them, but I think they give the promise. We have used them for other things.

Another example – maybe I will take the lead one because I think it is a good one. Historically, the public health department

receives every lead level check on a child who is a Chicago resident and any time a child has a lead level above a particular point, we automatically – nurses, inspectors are going to that home and working to identify how did that child get lead poison and correcting it. We, of course, want to be on the preventive side of that. It is about thinking where are kids coming in. They are coming in for well-child visits. We worked with a consortium of our federally qualified health centers, who are serving some of the higher-risk kids and said let us figure out a way here. Nobody has time to pick up the health department and call. Let us actually link the electronic health record to our registry and to our predictive models. The health department has built predictive models for a lot of things that we do. We use the predictive model to prioritize which restaurants we inspect. We use a predictive model to think about mosquito work. We are used to using this again with partners but using it in that clinical setting means again why did we collect this data, how did we build this because we want to actually have it mean something. We want to turn it into action.

The ability for a provider who is seeing a 1 year old well child check, for example, to sort of have an alert pop up that says this child based on the address without me having to do anything is in sort of potentially the highest risk for being in a household that maybe at higher risk for poisoning based on what we know. We do not know this child has it, but it would be a high risk.

You can then actually automatically put things in place that can protect that kid. You can do a proactive inspection. You can make sure you are checking lead levels earlier. That is the kind of thing we want to do. You think COVID or even Ebola – we were able to do a little bit of this with, for example, when we had travel registries. I think back to Ebola. There was a lot of hype around people were regularly coming into clinical settings and saying I have traveled here or I have this concern and maybe they did and maybe they did not. The ability to sort of quickly match up against a list that the health department may be keeping of people who actually have traveled within the time period and who needed more investigation. There are ways like in an emergency or in a nonemergency to link EHRs and the public health repositories in ways that protect – like I do not release this unless that person actually shows up and there was actually a need. That is what triggers sort of the look at this.

But we have done things like – we have done proactive stuff around people who have been found to have drug-resistant organisms, for example, and they are colonized. When they are

showing up at an emergency department, there is a ping that goes off and says this person, put them on infection precautions right now. There is a public health reason that in the clinical setting something different needs to happen. And that is very true for COVID. That is very true for any infectious disease. And we have plenty of ways of tracking syndromes, alerting things. The link between the clinical setting and the public health setting is important. It has to be protected and, in my opinion, can be much better used to help predict and alert people who need particular action taken. I think there is a lot of promise there and we have a few examples of having done it in the past.

As far as the infrastructure piece. I mentioned – I think this is really – this is for better or for worse, I think it is done pretty differently at different health departments. It is something here that we – I have a privacy officer, a privacy lawyer, who is really good, and this is his life work. And he is also the HIPAA compliance officer for the city. He is not the one who does our daily contracts and all of our regular law stuff. Literally, this is his only job. I think actually from a structural standpoint, thinking about whether it is through the public health law network or others like building up expertise and then placing it. I actually think at the local level is very helpful so that I know that I have someone who understands the patchwork of all of the different legal pieces and then can put that legal – he is somebody who will want to do the right thing, but wants us to make sure that we are following all of the appropriate precautions to do it.

I actually think sometimes it comes down to just having some of that expertise and then connecting those individuals so that I do think some of the best practices we have here. I know they are not done everywhere where a larger health department were able to sort of support some of that. It does not happen in smaller health departments.

But I think the local level here is particularly important because we are the ones actually interfacing with the patients with the health care providers. And it is not enough in my opinion just to do it at the state level. You have to make sure it is sort of getting down even if it is not a direct person at every local health department. Larger local health departments. I think supporting some of that work and expertise would be a great role or something that we could think about long-term or for smaller local health departments at least making sure at the state level some of that expertise gets through there because it is all about resources. Public health is not particularly well

resourced as everybody knows and I think this outbreak has made it extraordinarily clear.

We have made a particular commitment to having some expertise in this here. But if I have him, it means I do not have three other things I would like to do. I think it is a space for some more expertise and personnel to grow this as the technology grows especially.

Frank Pasquale: Thanks so much and, yes, I would definitely reiterate the point about resources because I think that is something that we really have to keep in mind. I think in my opening statement as well, I really was concerned about this resource point because I think we have to be willing to invest and not just in privacy, confidentiality and security and not just impose rules without that investment.

I see a question from Denise Love.

Denise Love. Hi. Thank you, Frank, and thank you, panelists. This was so interesting to me and my head is full of ideas and questions, but I will try to synthesize.

I was impressed with the work that each one of you have done especially in Chicago with the intensive work to effect the change. I think it lays out a potential roadmap for action.

But what strikes me is I think nationally what is going to hit post-COVID are all the unanswered questions that have to be answered. And we have these silos. And I think about the laws across the country, the vital statistics laws and others of the critical core data sets that are going to be needed on a macro-level. But many of these laws and use agreements were put in place in the 1970s and they are not going to suffice for the post-COVID or I guess intermediate COVID world.

But even beyond that, the culture shift in public health that has to accept letting the data go out to a broader audience and again the other points you hit on for the resource constrictions in public health generally.

Do you see the Data Commons as being a model that can be exported quickly, rapidly and deployed? How long do you think it is going to take? I guess I am worried for the rapidity of what we need versus the reality of what it takes.

Robert Grossman: Since it is addressed to the Data Commons, I will just make a couple remarks. First of all, I want to

emphasize what I call the swim lanes, that one slide, of which there are quite a few swim lanes. One is the public health swim lane. One is the hospital operations/patient care swim lane. There is a research swim lane. There is what data you need for governance. There is what data you need for community. You can build commons across those.

I focus my remarks on the last three swim lanes so they complement what is done in public health per se. They complement what is done for hospital operations. I think of this – all of us have to have a response to something like a public health emergency and we see this in sort of the nontraditional data-like mobility, the private projects that report on incidence levels and complement public.

We have been talking – if you look at the history, people have talked about persistent infrastructure for public health for a long time and we have that in terms of the modeling groups that has been supported in terms of the data collection. I would say that we do not have that in terms of the modern kind of tech infrastructure that could be used for this purpose and that is where I see an emergent need for infrastructure like the pandemic response commons, for infrastructure like apps that can be over time develop that balance privacy, security, and consented collection outside of the health care system. I really see it as sort of all the swim lanes have to get together. We have tools we did not have before. We have put in place some persistent infrastructure. But as someone who builds data platforms that sort of are used commonly from fintech to adtech to large-scale research, we do not see those platforms so easy to use for public health emergencies and I do not see any reason why they cannot be if we plan for this.

COVID is going to be around for a while, probably unfortunately as well as other variants. To me, I see this as a call. I wish we could have done it more quickly. I think it is going to be a shame if we are not ready in a few months for whatever we see with the flu season, et cetera.

Allison Arwady: And maybe I would chime in on that. I totally agree that these old – that we need some updating to all of the ways in which this is governed ideally. I will tell you that one of the biggest differences for COVID I think not just here in Chicago, but across the country has been that for the first time, CDPD, Chicago Department of Public Health, has stood up a daily, updating dashboard that was developed with community. We have percentages and rates are on there, but we have it in terms of – like if you look it up, it says one in five Chicagoans has

been tested for COVID. We have the rates. We have the more technical stuff on there for the EPIs. But it is also we have worked a lot to try to make it be very community understandable. You can look at it by zip code. Number one, that gets updated every day and it is fully transparent so that I see that data at the same time that it is available to the public.

And, secondly, it has eyes on it like we have never seen like hundreds of thousands of people visiting this dashboard, looking at this. And historically, CDPH – I have epidemiologists. I have data scientists. For most of our things, we would put out a report once a year. Maybe for things that were really hot like opioid overdoses. We do it once a month. That is just not going to fly, I think, anymore after COVID. People have gotten interested in public health data and particularly this local and data for action in a way that I think is very healthy and is going to be an opportunity to build it. But, boy, let me tell you. We do not have the data systems to do it. Right now, like I said, we have sort of had three to six months to try to modernize everything. We are just trying to get this sort off servers and into the cloud. We are just trying to build the pieces that need to happen around this and get the staff there.

But I think that it is one of the spaces. Like anybody in public health, federal on down, would have really pointed and have for years pointed to informatics and tech as just being a space that has not been invested in very well and it has kept us really delayed. There is the tech side in terms of investment, but also on the legal side and just the way these things have come through.

We, historically – we do not receive at the local level the vital statistics, the death stuff for a couple of years after they are done. And that is just not going to fly anymore. We have very much – in Chicago here, there is obviously a lot going on, but we are pushing sort of even at our state level to get some more modernized language into making sure local health departments, for example, have access to any of the data that needs to already be reported at the state or anything that is there, making sure that this can be available to locals, not in a way that adds reporting requirements, but opens this ability up for us to do more of this work.

With COVID, this attention and hopefully some of this investment in public health will be both on the tech side and on the legal data sharing framework. People often assume that public health does not want to release things or will not release things. Where we do not release things, it is because there are legal or

ethical reasons where we have privacy concerns that we sort of do not do that. But most of the time, we are actually pushing to have some modernization with the hashing and the tech and the other things that would allow us to share more of this, but there are often legal things in place that without some modernization keep us from doing that.

Those are the two – if anything comes from COVID like better – like this idea of faster, more available platforms with the tech pieces and the support for them matched with some of the opening up of even allowing local health departments to access and be able to turn some of that data into use at a community level would be fantastic outcomes from COVID.

Denise Love. And thank you and I hope through the discussion today that we can lead to maybe some modernization across the board to get the public health data more liquid that we need going forward. Thank you so much.

Frank Pasquale: Yes, absolutely. Great questions. Vickie, if you do not mind, I am just going to have one question for all panelists so then I will come to your question because I had one question for all panelists about – I just wanted to get a summing up from each panelist about your view about the role of exposure notification or contact tracing apps on mobile devices because I feel like – I have been part of different discussions where it just was unclear to me as to which was – whether these are a side show, whether they are something that can work in some health care systems like I really appreciated the distinction between Taiwan's centralized system and our non-centralized or if they are really an essential part. They can be a very essential part of public health response and that we really need to be thinking about them. That is just my question to all three panelists would be about the summing up sense of how important these apps are.

Ashkan Soltani: I am happy to jump in. I have said a lot about the topic already. I think it will ultimately depend on essentially what leadership we have in the actual public health sector on the use of these apps. I think a lot of the oxygen has been sucked out of the room debating the protocols particularly because platforms can generate so much attention and influence on what exactly the end product looks like.

I do think there is a role for public health agencies to really step in and say whether the APIs and the infrastructure in place are enough and too how they should be used. I think that has been missing. We have seen a lot of health agencies rush to

build their own tools and techniques and then slowly have to retool those approaches because of limitations on the platforms and essentially this nudge to use the new exposure modification API. And I am not sure that is the right outcome, but we have not seen folks publicly say one way or the other.

And my worry, as a technologist, is that there is not a lot of understanding of the actual underlying mechanisms. A lot of the folks are overworked and over tasked and kind of accepting on blind faith to what these systems will provide without asking the question of will they provide the thing that the health agencies really need like this outreach, this ability to track outbreaks, track clusters, forecast, those types of things. I think that is an important question.

Allison Arwady: Thanks. I would say a couple of things. One is that at the local health department level, my biggest challenge of all is trying to keep the trust of the public in the work that we are doing. And I think that in a conversation that has been increasingly politicized and that has so much misinformation out there and frankly people who are sharing misinformation about the goals of the health department and of the public health response at all levels.

I have had to deal with so much even where we have talked about – we have used, as has everybody, anonymized cell phone data where people have allowed apps on their phone to know what their location data is. We have used that anonymized data to understand things like how well did our stay-at-home orders – how well were people able to adhere to those. Where do have more essential workers? What did that look like over time? It has been very helpful for us to use some of that data to understand where perhaps neighborhoods are less able to stay home and what does that mean for our work.

But where we have talked about that publicly is it has often been poorly understood and has very much turned into the government is tracking me.

I am somebody who does direct. I do these Facebook lives like many times a week where I take questions directly from the public. And people are truly – there are people out there truly convinced that the vaccine is a goal for the government to implant trackers in their arms. And in that context, I certainly see value for these apps. I am excited to see their uses sort of in campus settings, in perhaps business settings, in some more closed settings where there is some consent implied in that if I am going to be an employee, if I am going to be a student that

there has been – like this is part of the practice of an organization that I have joined somewhat voluntarily.

I have not felt that from an adoption standpoint and all the rest of it. It is something I would be very interested in seeing be part of our sort of armament of response, but at the moment, I think I have been worried about stepping in too strongly because of the misperceptions about how this data is going to be used and how privacy is going to fill in.

I think that it is something that could have some promise and again I am really – we love seeing the way this has been done in some other countries, but the social way people understand privacy and the government's role is I would say just different here in the US than it is in a lot of other countries. And my hope is that we can get to a point where people can again trust that this sort of work is being done for no reason other than to limit the spread of disease. But my concern is that politically right now that is not where we are as a country.

I mostly am interested in trying to maintain trust and how we are using that data and I think it is going to continue to be just a huge conversation going forward.

I am hopeful that it will become something that is in the same way you share your location data with this app and this app and this app. Perhaps this idea of for public health has become something I could share I think is something I would love to see us get there. I just think culturally right now we are a long way from that and hopefully it will be something that grows out of this, but right now, it is something that I have trouble pushing hard as hard as I would like to because of the misinformation that is out there.

Robert Grossman: I am not going to comment on the -- I agree with Commissioner Arwady. Put it in context. I am not good at predicting tech future, so I am not going to try to predict the importance of the tradeoffs of contact tracing apps. But if I put my hat on as someone trying to work commons and swim lanes to improve health outcomes and to improve community response and to provide better data for decision makers, contact tracing apps is a third rail. It is not going to give us that much. It is not our swim lane. We simply ask the question with completely anonymized data that is volunteered without trajectory and private preserving. How can we get a lot of information that will improve the data we have and decision making without getting anywhere near contact tracing and whether it is fair or not?

There is a whole link for contact tracing. But what has happened is contact tracing apps, as was just described, have clouded the air and the whole thing is confusing now. There is a lack of trace. Our point of view is not only is there a whole separate link for contact tracing, but the confusion and the lack of trust makes it really important if you are going to bring the community in and leverage especially around things like health disparities that you stay very far away from those and it is just a practical thing.

Again, I am not talking about their role very broadly. I am talking about their role very narrowly, given the confusion around them right now. We just keep away from them – very far away from them or anything that looks like them or anything that people think looks like them.

And the problem is there are lots of apps. There are lots of apps collecting information. There is a lot of mobility information that is wonderful. But the fact that contact tracing app is not understood by most people actually confuses a lot of the things we need to do that have nothing to do with contact tracing.

Frank Pasquale: Thanks so much. And with the forbearance of Rebecca, if we could have your question, Vickie, and if we could definitely end by 11:35 that would be most appreciated. Thanks. Vickie.

Vickie Mays: Dr. Arwady actually stepped right into the question I wanted to ask about, which is trust. If Mr. Soltani could actually talk about this issue of how do we build public health trust in the use of technology. And are there any populations in particular that we should be the most worried about?

Ashkan Soltani: That is an excellent question. And I think you might – the way I would approach it is to disentangle. How do you build public health trust first and foremost? That involves both the communication piece, but also the brand piece and then relay that brand piece through the technology tools.

Right now, one of the challenges is in addition to the debate we are all having and the public health applications, for example. There is also a plethora of other apps that are COVID related, that are in different jurisdictions, that are different functions, but are all in the marketplace that make claims around being able to help people detect their symptoms or find local testing facilities. There is very little governance and branding.

We have seen a lot of scams, people calling in the UK, for example. People calling and convincing people that they are from the contact tracing authority and they need to pay money in order to get further information. There is lack of leadership authority and brand in terms of like who – is there a key tool or brand?

One of the challenges has been in the technology solution. At least the technology outpaced the policy responses in this regard. And what we had is technology kind of put forward the concept and the tools, but they have kind of left it to the health agencies to pick up the last mile problems so to speak. And that has not been done.

I think to the degree that there is a concerted effort and position that it can take the national level at the very least and then have essentially good communication guidance on what that is and then fill in the actual data piece with apps and tools and whatever technology piece rather than having the tech drive the effort. I think that would be incredibly valuable and then now what we are seeing.

And we look at places like Singapore and South Korea and others where the health agencies have taken a very active role from the onset and helped drive both what the role of the government is, the health agency is, and what the role of the apps are --

Vickie Mays: Thank you.

Frank Pasquale: Thanks so much. I think that we will now – I will defer to Rebecca, hand it over to Rebecca, but I believe we are now adjourned until 12:30. Is that right?

Rebecca Hines: That is right. Yes. I invite members to leave your Zoom on with the video and audio muted and we will see you all at 12:30 Eastern.

(Luncheon recess at 11:35 a.m.)

Rebecca Hines: Everyone has indicated they are back and I will turn it over to you to facilitate this next panel.

Panel II – Technology and Ethics

Melissa Goldstein: Okay. I would like to welcome you all this afternoon. We are very excited that you were able to join us for the panel on technology and ethics. We are looking forward to hearing from you all.

For those of you in general, the panelists are going to be Professor Danielle Allen from Harvard University, the Edmond J. Safra Center for Ethics, Dr. John Loonsk from Johns Hopkins University, the Bloomberg School of Public Health, and Kate Goodin, who is the director of Surveillance Systems and Informatics Program, Communicable and Environmental Diseases and Emergency Preparedness at the Tennessee Department of Health, and Stacey Mondschein Katz, director of Healthcare Privacy and Human Protections Administrator, Maine Department of Health and Human Services. Why don't we start with Professor Allen?

Danielle Allen: Thank you very much for having me. I am glad to be here. I think my comments will pick up several of the themes that came out this morning.

I am going to focus on technology understood in two ways, innovations and testing technology and then digital technologies and in particular digital exposure notification tools. I think both kinds of technology are producing challenges because they do not fit precisely in the structure that we have for addressing societal health issues whereby either something needs to be a matter of health care or something is a matter of public health surveillance. It is the fact that we have a lot of activity now that falls in some sense between those two categories that is producing, I think, our greatest challenges.

With regard to testing technologies themselves, as everybody knows, we now have many contexts, colleges and universities being the leading example, where people have undertaken routine testing of asymptomatic individuals and this is going to require some thought in relationship to how HIPAA is functioning.

Relatedly, digital exposure notification tools. They have not really gained significant traction in this country. In Europe, they have gotten penetration levels of approximate 20 percent, for example, in Switzerland, similar in Germany.

There, too, there is a new way of interacting with our health

systems that does not connect in a neat and tidy way to HIPAA.

What I want to suggest that both of these things – routine screening testing and these are things – the digital exposure notification tools are affected by category confusion that is affecting all of our responses – to COVID.

I want to clarify what I mean by referring to category confusion. The CDC currently is using three categories to talk about the role of testing and this is an extremely helpful framework. Diagnostic testing for symptomatic individuals or people with known or suspected exposure, screening testing, and surveillance testing.

The use of the screening category is still relatively new and vocabulary has not really stabilized around that category. For example, many entities are using a vocabulary of assurance testing to talk about routine testing in businesses and schools and the like. Of course, early on, we began routine testing in elder care facilities and that was sometimes categorized under surveillance. It is more recently that it is coming to be categorized under the category of screening.

And if you look at HHS categories generally and I know CDC is within HHS, but nonetheless if you look at HHS more broadly, HHS categories are really still just the binary of diagnostic testing on the one hand and surveillance on the other.

We have this third category that has emerged, screening, and that is where people are using and will be increasingly using low-cost tests whether it is the antigen test or soon to be available CRISPR test and the like. It may even be the case that people begin to use at-home tests. These approaches to testing are not straightforwardly captured under existing policies and regulations.

I would like to pull the way in which the categories do not fit practice now. As the CDC defines the screening category, the expectation is that screening testing is carried out by a CLIA lab. But in actuality, we have colleges and universities and businesses and schools and third-party providers that are conducting screening and are not necessarily CLIA certified labs. Again, if we have do-at-home testing kits that too will be a kind of testing that is not done in a CLIA lab.

Ultimately, for the volume and rate of screening testing that we need, we cannot expect all that testing to take place in a CLIA lab, which means we have to revisit the question of how to

ensure that IPAA applies in these contexts.

Let me turn to that specifically for this category of treating testing. What are the relevant privacy issues? First of all, I think it is pretty straightforward that a screening testing even of an asymptomatic person should fit within the definition of health care services as is articulated in HIPAA. The language that HIPAA uses there is as follows. Health care means care, services, or supplies related to the health of an individual. Health care includes but is not limited to the following. Preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling service assessment or procedure with respect to the physical or mental condition or functional status of an individual or that affects the structure or function of the body. Screening testing pretty clearly fits under that definition of health care. However, the entities that are providing that screening do not fit under the definition of covered entities under HIPAA.

What this basically means is that we do need clarification that HIPAA applies to screening testing sites because of the definition of health care and that we therefore need to broaden the list of HIPAA-covered entities.

If we could do those two things, then we would bring a whole lot of the activity of testing into a HIPAA-covered framework and that would significantly advance privacy protections.

Of course, in doing so, it would be important that there be public education that HIPAA is consistent with sharing of data with public health authorities in the context of a public health emergency. But the good news is that HIPAA already has the frameworks that we need to balance protection of individual health information rights and public needs.

In that regard to the degree that as new practices develop, we can adjust our frameworks to incorporate them under HIPAA we are better off.

A related issue with regard to data and data management is that we need clarified norms for when screening positives should be confirmed with diagnostic testing. And the reason this matters is, of course, that the diagnostic testing processes are all well integrated into our public health systems. It is not clear that screening testing is as well integrated.

That problem is solved of course if positives require confirmation with diagnostic testing. But right now, there is an

absence of norms around that and that absence of norms around practice there actually affects how data flows and how it is integrated with our health systems.

As an aside just because you are a group of informative, important people, I want to just note that we also need clarification about payment systems for screening testing precisely because this category is a new concept, a new category for us, and it has a large volume of activity in it. Many of the problems about funding testing directly relate to the fact that this category falls between the stools of insurance and health care coverage and traditional public health ways of funding things.

In the same way that screening testing and the data that is connected to that falls between the stools of health care and traditional public health, similar, the same is true with the payment systems. We need to actually rethink both our privacy regulation and our payment systems for this new category of screening testing.

Now, let me turn to how this category pertains to exposure notification technology. Here, I am drawing on a paper, one of the white papers in our rapid response series of the Edmond J. Safra Center for Ethics. This paper was spearheaded by a team from New America, the Open Technology Institute. Sharon Bradford Franklin was the lead on this project. And this project really looks closely at the privacy issues related to exposure notification technology. We heard a lot about that earlier. Again, the European countries, many have coalesced around Bluetooth-based technology, the Google Apple. API also has coalesced around that Bluetooth technology.

This use of exposure notification is in contrast to screening testing, not a health care service. So providing information of potential exposure, there is not any direct assessment or service related to the individual’s health. In that regard, the notification tools do not make sense to fold them into HIPAA coverage. We need an alternative approach in this instance.

In this white paper, this team, our team recommends two things in particular. Federal legislation and also resources to the FTC and state agencies to hold companies accountable for any privacy violations or other deceptive practices.

The most important thing to do when looking at this is to spell out precisely what the right principles would be for any legislation that might provide safeguards to hold governments

and companies accountable.

FTC and state agencies can hold companies accountable even in relationship to their own statements, their aspirations. Google and Apple, for example, both describe what they built as privacy protective, privacy preserving. So they have to be held good to that. If there are violations of the privacy protective elements that they built into app or they actually fail to deliver on that, the FTC could hold them accountable for that.

Let me just focus now as a final thought on the seven principles for legislation that Sharon Bradford Franklin and her team articulate in this paper. Meaningful consent. All participation in contact tracing. Applications should be voluntary. That should be a basic thing.

Voluntariness requires that participation is not a condition for access to public benefits, work, or educational spaces. And companies must obtain meaningful consent to collect and use personal data. The notice of consent model – characterized privacy enforcement the US – fails to protect user privacy under normal conditions and should not be the consent model used here. The stakes are higher.

The second principle is transparency. App providers should be fully transparent with users by the type of data collected. The entities all have access to the data and how data will be used. And Congress should require notices to be accessible to those with limited English proficiency and to be available to machine readable format.

Data minimization. I think you heard a lot about this earlier today with the discussion of the Bluetooth app so I will not say much there. But it matters that only the types of data necessary to support the very precise public health needs should be collected.

Limited retention period. Data should not be retained by companies or public health authorities indefinitely. And legislation should define the retention period for personal data. That legislation could permit longer retention of aggregate anonymized data by public health authorities for research purposes.

There should be a prohibition on secondary uses. The data should be used for public health purposes, not for commercial purposes such as advertising. Nor should data be shared with other governmental entities other than public health authorities. For

example, there should not be any sharing with law enforcement.

Data security. Companies should maintain best security practices to safeguard the collected data. Decentralized implementation is key. And, again, we are seeing the value of that in Europe where those countries that chose a decentralized model have had much more significant uptake of the apps than the countries like France that pursued a centralized model. Also, de-identification methods like differential privacy and encryption are critical.

And then finally, equity. Companies should take steps to prevent disparate impacts of uncertain populations of demographics and that should include a prohibition on (indiscernible) uses of the data. I know there is going to be another panel on that subject later, so I won't say more about that now. But these are the seven principles that we would recommend for any use of exposure notification technology.

All that said, I do think that this piece is a smaller part of the puzzle than the first piece. The need to fold screening testing into the HIPAA protocols. Screening testing is already increasing in volume. It will increase in volume. It is a critical already active tool for suppressing COVID. Perhaps our most important tool.

Ensuring that that activity is carried out in accord with HIPAA policies I think is task number one. Exposure notification technologies. I honestly do not expect to achieve huge penetration in this country over the course of this pandemic. I think these principles matter for establishing legislation that will help us prepare for the next pandemic so we will want them for that. But I think the former issue is the more important one for the next three to six months. Thank you.

Melissa Goldstein: Thanks so much, Dr. Allen. Dr. Loonsk, could you join us now?

John Loonsk: Thank you for the opportunity to talk about some of the aspect of public health surveillance that I have been involved in for the last several years.

I am with Johns Hopkins, but I am also the Electronic Case Reporting lead for the Association of Public Health Labs. Electronic Case Reporting is the context in which I am principally speaking to you today.

Electronic Case Reporting is the automated identification of reportable health events in electronic health records and their

transmission to state and local public health authorities for review and action. This has been very prominent in COVID-19 by the Electronic Case Reporting only really was being initiated at the start of COVID-19. It is a joint initiative of the Council of State and Territorial Epidemiologists, the Centers for Disease Control and Prevention, and the Association of Public Health Labs, a real acronym soup there.

What was pointed out in COVID and has been true in many outbreaks before COVID is that there are critical clinical data that are necessary for doing outbreak management, supporting contact tracing and supporting other operational activities in state and local public health agencies.

There has been an effort in COVID-19 to try to extract these data from lab ELR, electronic laboratory reporting, but mainly they come from clinical care and they come from clinical care systems and electronic case reporting, eCR, presents these data in a way that they can be electronically consumed by the public health agency.

As I mentioned, we were just beginning to roll out at the start of COVID-19 and we had three initial implementations after this project eCR had been incubated in the Digital Bridge initiative for some time.

After the start of COVID-19 with an initiative we call eCR Now, we have promoted the importance and advancement of electronic case reporting for COVID-19 specifically and we now have over 4800 sites that are doing electronic case reporting for COVID-19. Variable explosion of activities driven almost exclusively from the provider space wanting to do the right thing and advance the data that needed to be reported to the appropriate public health agencies.

Case reporting versus electronic case reporting, but generally case reporting including COVID-19 now exists in all states with the support of HIPAA. It is ensconced in state laws and it requires identifiable data to be reported to public health agencies without patient consent.

We had developed an all-jurisdiction, all-condition electronic case report standard, the eICR, that data for which were identified by a taskforce of the Council of State and Territorial Epidemiologists that said that these are the data, this set of data are what are appropriate to the advanced in a case report to public health agencies. We have authored and

there are available over 89 conditions now, but the focus during COVID has obviously been on COVID.

The activity of electronic case reporting has been greatly aided by partnering with the eHealth Exchange and now with Carequality. And the outcome of those partnerships is that all eHealth Exchange members, Carequality implementers and even CommonWell members and all those that connect to each of them can do electronic case reporting without any additional data use agreements or other legal agreements. This is substantially enabling of the advancement of electronic case reporting for the COVID-19 purposes, the Carequality implemented and Electronic Case Reporting use case during CoVID-19. We had a partnership with eHealth Exchange before it, but this factors into other considerations that I will return to.

Part of the issue here is that Electronic Case Reporting while in process – it has not been effectively advanced by federal regulation and is only a menu choice in CMS' Promoting Interoperability. And many choices particularly at the end stages of meaningful use have not been effective in achieving broad implementation. As I said before, 4800 sites that are reporting now. Almost all of them have commented that the behest of the provider organizations wanted to do the right thing and advance this activity electronically and get rid of manual reporting in the process.

There has been discussion during the course of COVID-19 about the fact that public health agencies may need broader authority to collect data – important to point out that in the context of the process I expressed to you that these suggestions are not generally cognizant of the eCR data yet. eCR is new. The data are broad and appropriate for case reports, but many have not yet experienced them at the start of COVID-19 and not yet integrated them into their traditional surveillance activities.

Some though have suggested that on the basis of needs from public health agencies that they should be enabled to get other documents like the CCD so that they can utilize those instead.

The unfortunate part about that is that the CCD and other clinical documents do not have all the specific data that public health needs. And two, there are some clinical data in CCDs and other clinical documents that public health is not eligible to receive or really want.

The take home from this for me is that these issues of data availability at the public health agency are more a factor of

inadequate advancement of existing public health requirements and authorities than necessarily the needs for new ones. I am specifically talking about case reporting. There are other activities around hospital capacities. There are activities around electronic laboratory reporting. But in the context of electronic case reporting and what we would call epi-data or clinical data, these statements ring true.

We need more federal incentives and support for state-based programs like eCR to advance the appropriate delivery of existing data enabled by HIPAA to achieve support for those public health agencies. This is more a problem of omission rather than commission and it is an issue that hopefully can be rectified moving forward to make this necessary function electronic case reporting something that is indeed required for all health care organizations to participate in.

The other major point that I would like to get to is in the context of the role that health information networks have played and where TEFCA can play going forward. In COVID as part of the electronic case reporting, we have really seen the power of a nationwide health information network broadly. I mentioned that we had a partnership with eHealth Exchange. We added care quality. That brought in CommonWell. And essentially, that is a lot of the TEFCA vision for a policy framework that would be enabling of appropriate activities, but also potentially apply appropriate security and consideration at the same time.

The eHealth Exchange DURSA and the trust agreement in Carequality facilitate the exchange of data. But with that policy scalability, also comes the ability to have the related security and transaction validation that is needed in many public health activities. Public health reporting is a first transaction, data actively being sent from clinical care to public health agencies. That is what I have been talking about.

A second transaction is potentially public health investigation, which may take more of the form of a query. The determination of the data sets that are involved in those particular activities include for reporting the data set identified by the Council of State and Territorial Epidemiologists. What we have seen during COVID is the opportunity for public health investigation is very much mediated by others in the health IT milieu, EHR vendors, and others and really careful consideration has to be given to how these network capabilities going forward should be validated and blessed from a data access standpoint so they can both meet broad privacy policies and be in keeping with the data needed

for a public health activity as well as to ensure that the data necessary for public health are actually available as required.

Thank you very much for your attention and look forward to comments and questions.

Melissa Goldstein: Thanks very much, Dr. Loonsk. Ms. Goodin.

Kate Goodin: Yes, thank you very much. Hello and good afternoon, everyone. My name is Kate Goodin and I am with the Tennessee Department of Health, but I am here today speaking to you all on my role on the executive board for the Council of State and Territorial Epidemiologists, which if you are not familiar is a professional society, representing those of us in applied epidemiology at both state, territorial, and local health departments.

I know that we are here to speak about COVID, but as several people have mentioned throughout today, there are a lot of implications for how some decisions made here through this committee could affect other future responses. I think part of what I would like to do is take you a little bit back into history and talk through some of our other more recent nationwide public health issues to emphasize and maybe reemphasize some of the differences between how these responses rolled out across the US and what they meant for state and local health departments.

Here, I have included a few headlines of notable situations, which may have come to your attention at a national level, but small versions of these responses occur on a daily basis at state and local health departments across the US and they all bring unique challenges with regards to medical and clinical information needed, the partners, public health agencies are working with, and recommended prevention and mitigation efforts, which each inform the public health view of data sharing, disclosure, publication, and privacy concerns.

For example, in the large national fungal meningitis outbreak in 2012, it was necessary to track patient medical history for a significant time prior to those individuals becoming ill. This was necessitated by the extremely complex medical histories of the patients who typically received the type of steroid injection that was ultimately implicated in this outbreak. This is similar to the type of response needed in 2019 when clusters of lung illness were identified in the US and vaping was implicated. These types of responses often include medical imaging, medical record review, patient histories, which all

come from that clinical sector, and then patient and family interviews or directed lab testing, which are collected by public health staff.

Food-borne outbreaks are much more straightforward in many ways, especially related to privacy concerns because public health officials are often looking for very little PHI simply demographics and the specific lab results, which diagnose that condition. However, they often generate the most public and outside interest because of the food exposures implicated. Was it a specific restaurant? Was it a specific food like cucumbers, lettuce, cilantro, all of which have been implicated in recent outbreaks? Was the item all sourced from a particular farm and what that means for communications, disclosures, and that sort of thing?

Different agencies, entities, and the public have a vested interest in this information to both protect them and their families by things like potentially throwing out those contaminated food items all the way up to improving farm production, transportation processes within the agricultural industry and things like that.

What level of data and information sharing is appropriate for this situation? What if public health authority were only about 70 percent sure that cucumbers were the culprit in this outbreak? What if they were 60 percent sure and how does that define what you can and should share?

There is a similar issue around I think about 2008 with an outbreak that was originally associated by public health officials with tomatoes, which basically decimated that entire farming industry for about a year. In the end, those cases ended up being conclusively linked to a different product, cilantro.

Responses to Zika and Ebola brought up new issues for data sharing and privacy within the public health sector. For Zika, the vector is a mosquito, which meant that individuals could be at risk for acquiring the disease without being aware. This necessitated some unprecedented public sharing of locations of homes and work locations of individuals confirmed to be Zika positive. This was linked, however, to a very clear public and individual action set such as people in the surrounding areas, limiting outdoor exposures, preventing mosquito breeding in their backyards as well as pregnant individuals taking perhaps some more additional severe restrictions, obviously voluntary.

On the other side of that coin was the rabid demand for specific individual-level identifiable information on suspected Ebola cases. Someone previously mentioned returning travelers and all of the large infrastructure and effort that went out that as well as people returning from those affected areas.

At the time I was at a local health department and we had schools and agencies calling us for the names of those responding staff so staff from the US who went to staff these Ebola treatment facilities in the affected area. They wanted names of these individuals so that their children could be excluded from school or spouses excluded from work, none of which was based on public health or medical recommendations.

The stigma experienced by residents of African origin or suspected origin were extremely intense around that time on whether they traveled to Africa or not, whether they traveled to affected countries or not. It did not seem to matter.

I would also like to mention the large number of public health responses, which again we operate through on a daily basis, which do not require identifiable data either at or through the public health agencies. One of them is listed here.

Many of these types of responses include monitoring impact of environmental exposure such as wildfires, hurricanes, poor air quality days, and other similar issues, using aggregated data as its appropriate at this time.

I will start out also by saying that I am in no way a lawyer. My discussion around legal issues in public health is really more from a practice-based experience – before going into what we are talking about here.

But it is really surprising on a daily basis how many individuals, agencies, businesses, profession types are not aware that public health agencies are authorized to collect identifiable clinical information, including demographic, medical history, diagnostics, medications, and others and data is necessary for public health agencies to carry out our mission to control diseases in the community.

These requirements for disclosure to public health are authorized through several critical, overarching rules, which have been discussed previously here today so I am not going to belabor them. But they do define not only the public health authority to collect that data, but also provide some guidance

on how we should be receiving that data, how we should be storing it and other conditions.

In addition, most public health entities are more directly defined by state or local health statutes, codes, and rules, which again some of which have been mentioned here today. But each state maintains a statute, which again compels this reporting of specified conditions as Dr. Loonsk said earlier. And these statues often specify the content of those reports, the method of reporting, and the authority of public health entities to access medical records. For example, in the state I am working in now, Tennessee, medical providers and hospitals are compelled to provide access to certain medical records and any hindrance can incur a fine so it is a state-based rule for access.

North Dakota has statutes which criminalize the disclosure of PHI to the public of non-covered entities. Florida, at the time I was working there, had a statute, which disallowed the direct data sharing from health providers to any entity outside of the state. All data needed to go through the state agencies so at this time the Department of Health prior to any national warehousing.

Many of these statutes also directly relate to specific data streams or data sets. For instance, in Arizona, the cause of death is statutorily confidential and cannot be released. Fact of death can be confirmed in many cases, but how and why the person died cannot be disclosed even to coordinating public health agencies, meaning local health departments, internal – response groups and that sort of thing occasionally have difficulty accessing fact of death and cause of death information in emergency response.

HIPAA can also apply to state, local, and tribal health departments in different ways. Public health entities are generally classified as covered, exempt, or hybrid. And each of those designations can have profound implications on what information can be shared and disclosed outside of the health department. Even they can differ within a state or a jurisdiction depending on that public health entity.

One of the things that we also genuinely are concerned about on a daily basis is the HIPAA penalties assigned for violations and it is a little bit confusing to state and local health departments where those liabilities fall when a public health agency provides data to another entity such as that public health agency sending COVID data to HHS or CDC during the

current response and that entity subsequently discloses that data publicly.

Is the originating public health agency absolved like in the case of North Dakota? Would then their state agency fall under those criminal penalties or what about with or without a contractor or data sharing agreement and how does that affect liability and practice?

Public health entities also exist within a set of ethical principles, again, which have been mentioned earlier and governor actions beyond the letter of the law or statutes. These are heavily influenced by the history of medical and public health practice in the US, some of which are listed on the screen.

When it comes to how that is represented in data collection and sharing, we often ask ourselves things like is this particular data element essential to collect. How might my analysis change if this value was included or not? How does this value influence my surveillance goals?

I am interested in looking at COVID exposures for a case. Is it necessary to collect their Social Security Number? Many times, maybe not. Is it necessary to collect their birth city or birth state? Likely no, but the answer could be yes if we were asking about a long latency of cancer of something like that.

Similarly, we ask ourselves if knowing that information would be actionable. What is the public health action which would be compelled based on having this further information? What public health actions could be compelled publicly if this data were disclosed? This is much like the Zika example from earlier and then there is definitely a lot of gray areas of maintaining the public’s trust, which has been mentioned extensively here today.

Do they trust that we are collecting the right information for the right reasons and the same for disclosures? Are we disclosing the right information for the right reasons?

Although public health agencies are governed by the law mentioned previously, the public is not compelled to interact with us. They can easily refuse to participate in a food exposure questionnaire. They can refuse to name their sexual partners in an STD investigation. Although there obviously are some exceptions for different public health control measures.

This question becomes a really practical challenge for public health agencies. That ability to maintain trust and public health response is sometimes often countered to the interest of another party involved in the situation. For example, in the food-borne outbreak scenario, is it more trustworthy to disclose a restaurant you suspect might be linked to several illnesses only later to find out that it was a food product distributed to dozens of restaurants or a wait for a couple more weeks to receive back laboratory criteria thus potentially allowing more people to be exposed at these food locations?

Is it more trustworthy to disclose the locations of all Ebola-exposed individuals to ensure that the public is aware and can avoid contact with them or to protect those individuals from public scorn for something that you deem to be of no public health risk.

I will also comment that during the current COVID response, people are refusing to provide information or outright hanging up on investigators at a much higher rate that I have ever seen in any public health response to date.

What you see here is a diagram, which is I am sure pretty familiar to all of you. It is one of dozens of different diagrams of what a health information exchange flow might look like. What might appear unique from my perspective here is that public health exists on this diagram at all. As federal programs like HITECH and meaningful use rolled out, public health was often an afterthought and not seen as a priority for investment of time and resources for those developing these technologies and interfaces and Dr. Loonsk previously outlined a lot of those implications for eCR.

If public health is considered at all, we are also seen as an endpoint, but information is sent to health department or governmental agencies, but that the relationship is never bidirectional. This is true from the perspective of many public health practitioners as well like why do we need to provide our STD testing results or immunizations provided to the HIE if all that just happens is that those records come back in a circle to our registries.

But this view also ignores the role that public health agencies play as part of the health care continuum. As health care and technology projects or policies are pursued, we should be asking ourselves routinely where is public health in this project, where is public health at the table. Is public health getting the data they need? Is it timely? Is it complete? Some already

established methods of communicating to public health or electronic laboratory reporting in addition to case reporting, which again was previously mentioned.

These standards have existed for years or in the case of ELR for over a decade and need to continue to be emphasized. As the COVID response has demonstrated, many within the heath care sphere are still not yet aware of these standards and reporting initiatives and moving them towards greater implementation is pretty critical for our public health response.

Public health being a capable, interoperable partner has also become a particular issue in the COVID response as many payers and provider organizations are requesting COVID testing results for all tests performed within the state or jurisdiction. They would like to know, for example, if a person was tested at another site through one of the pop-up testing locations or drive-through testing locations offered through health agencies or through drive-up pharmacies, for example, locations that are not likely already participating in their data networks.

This has presented a particular challenge for public health agencies, given the obvious utility of knowing this information as part of their clinical care. We have never provided identifiable health data outside of the public health agency in most cases. That process is very unfamiliar to state and local health agencies.

Additionally, what are the data privacy obligations owed to those data providers? Originally, if we were receiving electronic laboratory reports from hospital systems or commercial laboratories, what are our obligations to them as a data provider? What does our insurance partnership providers need to know about the services that an individual member has received outside of their network and outside of their payment structure? These are challenging questions that public health agencies are currently facing and do not have ready answers to. We are also looking for best practices for future public health responses. How do these questions change depending on the type of threat we are facing?

All my previous comments presuppose that the required and desired information is even received by public health and that is just not reality. What is reality is what I have on this slide here, which is lab and case information that was faxed to public health agencies and my public health agency in particular, obviously removed of any identifiable information, which has nothing to indicate where this test was performed so

no test location. We have no idea what facility completed this test. There is also no explicit information about the type of test performed unless you are intimately aware of what the ID NOW machine is which it does mention here. You would not know what test was performed.

This reporting issue of facts reports of really low quality of readability with really low quality of content definitely pre-dated COVID, but it definitely has been exacerbated during this response as the number of providers and testing entities has ramped up.

These facilities are not capable of integrating these instruments into their EHR and that is not across the board. That is for particular sectors or into their lens system if they even have one. And they are definitely not able to send their EHR lens data in a structure message format outside of their system.

We have had several facilities that are having to read results that have a human's eye read results from a point-of-care test machine on the display and then hand enter those results into an Excel sheet in order to have any sort of record for patient-level results, not just for reporting.

These machines do not include out-of-box interoperability and has become a large barrier in both their operational use within the clinics and then for public health reporting.

There have been decades of federal incentive programs to support HL7 messaging between organizations, HIEs and public health. But the majority of the organizations where we are connecting for with the COVID response have never heard of these standards nor have they considered electronic data exchange of any sort.

This is not exclusive to facilities new to lab testing. Some large hospital and health care systems have not seen public health as a priority for interoperability and are now struggling to catch up to meet our COVID reporting regulations.

When your committee is reviewing all this to move forward with your guideline development, I have this list of groups here that are relatively generic. But all of these groups at some point throughout the COVID response or previous responses have requested identifiable case-based data.

For the most part, state agencies were not able to comply with these requests nor should they have. But it is something to

think through as far as who should be receiving this data, how should they be justifying it, what agreements need to be in place, and how can we ensure that public health authorities again are balancing that need for individual privacy and security with the public's good.

How do all these pieces play into the recent moves towards more open data policies, technologies, allowing aggregation and visualization of disparate data sets and all the new methods for processing these large data sets?

I think for all the reasons I stated previously, health data disclosure needs to be purpose driven whether the data sharing is for the patient, from the patient, their medical provider, or from the public health agency to federal or public partners.

The need for information from patients and medical providers should be clearly articulated by public health partners and I think I have outlined many of those uses here.

However, when we get outside of the potential benefits that patients or their direct community similar to what we are all considering human subjects research, the risks of disclosure begin to outweigh the benefits of potential analyses.

Many people have argued that there are often public interests in the data and that that is sufficient to justify disclosure. I am not going to get necessarily into my views on that particular argument because it would take a lot of discussion. But I would ask us all to think about whether we would want the – level information of our personal STD tests or drug overdoses publicly available. The same for our children. Would we want their STD information publicly available? How does your reaction to those questions differ given that we are speaking about COVID instead? Again, thinking about how – what you provide as guidelines could differ based on the type of public health threat being faced.

There are unprecedented levels of data being released locally and nationally on COVID with a corresponding nosedive in public health's ability to collect information from cases and contacts. I really do need to emphasize again that the number of hang ups and refusals for interviews is higher in this response than I have ever seen in anything in the past.

Some version of the old saying goes is just because we can do something does not mean we should, which I think I have already covered my thoughts on the reasons why we should not disclose data under certain circumstances. I would also flip that around

in the context of public health data and say that just because we should collect or share something does not mean that we can. Those limitations are typically related to whether people are compelled or required to report the information as well as whether the technology exists to do that same thing.

Today, I would say that the state of reporting to public health agencies means that we likely cannot meet the needs of our own agencies or outside partners. Thank you.

Melissa Goldstein: Thanks very much, Ms. Goodin. Ms. Katz.

Stacey Mondschein Katz: Good afternoon, everyone. I am Stacey Mondschein Katz and I oversee Privacy at the Maine Department of Health and Human Services.

Just a brief background on who we are at the Maine Department of Health and Human Services. We really are a conglomerate of offices and programs, including licensing, the CDC, various health and welfare entities for aging and disability as well as behavioral health and children's services. We are the gateway for assistance, nutrition, and temporary assistance for needy families. We also have the Medicaid agency and we oversee two psychiatric facilities as well.

As mentioned before, within the categories of entities, we are a hybrid-covered entity. Within our umbrella, we have HIPAA-covered entities such as MaineCare in our facility as well as the Maine CDC, which has – its single-covered entity is a portion of the Health and Environmental Testing Lab, which tests human specimens including the COVID-19 specimen and otherwise would be considered a public health –

We have a strong framework and really my presentation is focusing on the human factor involved in the privacy and security space. We have privacy and security liaisons to me and each of our offices. And we emphasize training and education, policies, forums, protocols. We have a web page. I send out regular emails for reminders. We have a relationship with the Office of Information Technology, which really serves as our technology arm. Internally, we do not manage our own technology space, but we are in regular communication and work as partners. Additionally, we have regular communication with our workforce on privacy and security topics and there is a knowledge of how we proceed in terms of any sort of incident around breach.

While we maintain our own across the board privacy and security policies at CDC, it additionally has its own and will suppress

data where numbers could identify individuals and small communities. And being in Maine, there are a number of small communities so that becomes more of a factor.

In addition, we have a research process so where people outside of the department are asking for data whether it is from the CDC or from the Maine Department – excuse me, from the Medicaid office. They need to go through our research process so that we can track the flow of information. We ensure that it is reviewed by our IRB of record and/or at our HIPAA Privacy Board, where appropriate.

In terms of the COVID test results here, so the laboratory tests that were obtained by the health department are kept secure in their Starland system and those are protected by administrative safeguards such as policy and training, physical safeguards, badge security to enter the facility, technical/system security from our perspective would be password and so on and then from the Office of Information Technology would be handling things such as virus protection and firewalls and so forth. And, again, when anything is sent from the lab to of course the provider that becomes part of the HIPAA-covered record. And when those results are reported by the providers outward to perhaps our disease surveillance program inside the CDC, as mentioned before, there are so many silos and so many laws, it becomes very complicated for folks. But when the physician sends the testing out to the public health authority to the disease surveillance program that becomes no longer covered by HIPAA but covered our state law and other protections.

Following the flow of our lab results after the patient has tested and the information is transferred from the laboratory emerged into the National Electronic Disease Surveillance System, NEDSS, that information is used to identify confirmed cases and then case investigators follow up on those confirmed cases and then to obtain close contacts as well as to find out about needs and social needs, et cetera.

The close contacts are transferred from NEDDS to the SARA ALERT system, which is hosted by the American Public Health Laboratories. Again, all of these meet our security standards and OIT, our information technology security standards. And the contact tracers, using the SARA ALERT, will reach out to contacts by phone, seeking to enroll them with permission into the contact tracing system, allowing the individuals who are being traced to put their symptoms into the system through their phone and so on.

When either the case investigators are contact tracers are reaching out to folks who determine they need additional services, they receive or will receive permission before sharing that information with the commissioner's office, with partners, and contracted agencies who can help fill those needs.

The CDC has a webpage that updates a dashboard on a daily basis. Then we also share our information through the news media. Dr. Nirav Shah is our public face, the director of the Maine CDC. The information is used for case investigations and it is used for public health activities, surveillance, containment, analysis.

This is Dr. Shah. When Dr. Arwady mentioned the concept of trust, I have to say her mentioning her regular Facebook discussions and so forth. That made me think of Dr. Shah. He is a regular face and he is basically sort of the vision of trust for the department in terms of the CDC. I have even seen T-shirts that say keep calm and trust Dr. Shah. He has been a really good and integrity-based word for all things related to COVID-19.

Of course, in order to use information, our best practices to de-identify if it is going to be made public in any way. By stripping information that is HIPAA best practice to de-identify by taking out 18 identifiers and anything that could reasonably be used to identify or the covered entity does not have actual knowledge that combined with what remains that a person could be identified.

This is an image of our daily case posting. The cases are posted by county. Initially, there was hesitancy to post information by county, again, because there are small counties in Maine. There is a lot of concern about whether or not this would identify individuals. But they are posted by county and going on a daily basis.

We also have a map posting by zip code and this is where we will be suppressing the numbers where they fall below a certain value because there are some very small communities.

And then on a weekly update, there is a posting to protect the privacy of individuals in small communities insofar as it speaks to age and race and ethnicity. The concern is that a regular and daily posting combined with other postings could simply identify individuals – Maine is not a highly disparate – it is a pretty homogenous state and growing in diversity. But in order to

protect the identity of individuals, the determination has been to make some of these categories posted on a weekly basis.

In terms of ensuring that human factor case investigators, contact traders, we want to be sure that they understand what they need to do in terms of confidentiality. They are required to have training with me either live or through recording.

And then in terms of user access to COVID data in our systems, protections include whether a person can access, for example, the health information exchange for this limited purpose. That information is audited for appropriateness.

Again, the case investigators and contact tracers have been educated on the sensitivity of privacy and security issues. This could be any of ours staff. Reminders that they are going to have access or very likely they have access to information about individuals they know from community, school, and work and that has been brought to my attention that a person who is a contact tracer who has been a nurse in a community was on the phone with someone who they knew. And they need to be very gentle and ensure that those individuals receive the exact same protections and that there is no misuse of that information. The minimum necessary information is used exclusively to get the job done and that is to ensure that the person is receiving information that is needed for either the contact tracing or case investigation purpose.

And then people understand who they need to reach out to in the event of any type of privacy or security concern or incident. They reach out to the privacy or security liaison inside of the Maine CDC who is a liaison to me and that is how we move forward.

From my perspective, there has been an extraordinary conversation this morning about the various and sundry initiatives and technology systems that are in place and may need to come into place to move forward in a public health space. However, from where I sit, one of the biggest risks is around human error in light of the pandemic. We are working from home. We are working from a variety of locations. We are moving between office and home. We have our children. We have our dogs. We have personal issues that are happening, and we need to be very careful in terms of how are we handling data.

I try to remind everyone and I think it is very important that this be woven through any information moving forward that our workstation is wherever we work and that our privacy and

security safeguards apply whether we are using a home, fax machine, or we are trying to discard documentation, et cetera.

There has been mention around contracts and data use agreements. We also have something like a data use agreement, which is a HIPAA term of art. We tend to call ours a Data Sharing and Protection Agreement. These are executed for the purpose of providing supports and services through our agencies in the research context and more.

We ensure that our templates ensure that there is consumer confidentiality language, agreements not to re-identify, agreements to contact us, contact me, contact the department within 24 hours or 1 business day and a promise to work cooperatively with us if there is any kind of risk, investigation, or incident investigation.

From the lab standpoint, since the lab is a hybrid entity within a hybrid, much of what it tests is not HIPAA covered, we do have a HIPAA business associate agreement, a template agreement that is required for people who are working to extend and enhance our COVID testing capacity.

There is health information privacy training for any new contracted workforce. There is a department review, for example, of our security controls to ensure that our access and our termination provisions are strong and secure. All of these whether it is HIPAA covered or there is state law covered, whether it is covered by a state rule, we basically take the umbrella and put it over all the data that we have. We have vast quantities of sensitive information and as has been discussed earlier today, people are not always clear that HIPAA either does apply to their public health information or does not apply. From our perspective, we try to take the strongest protections and put them as an umbrella over all of the information. But during this pandemic and during this public health emergency, clearly the public health use is much more extensive and certainly permissible by law.

We have limited access now to the statewide information exchange during this pandemic to assist with containment as had been mentioned earlier of how public health entities generally are not engaged in the health information exchange. In this context, we are permitted to provide – obviously, we are providing providers – the exchange allows providers to view patient information or consumer information, but it also permits the CDC and certain of our contracted staff to access consumer

information and consistent with the emergency rules for the purpose of containment.

And that access is very closely audited and monitored. Any questions around any sort of access by any of our staff or contractors is brought to my attention immediately and we follow up.

And often it tends to be really just a miscommunication in terms of where a person was permitted to view for the purpose of their role, but it is very closely and tightly contained to ensure the confidentiality of the consumer information.

In summary, as we are working from my space in the human factor, I oversee the work of the thousands of people who work for the department and now expanding to our contractors.

I try to remind everyone that we need to slow down. We have our hands in so much data and we are moving very quickly. People are making errors just by misfiring information or keeping information open at their kitchen table with their teens around, et cetera. We want to ensure that we maintain all of our safeguards as we would in an office setting. We want to ensure that the protections are documented in terms of any of our contractors with appropriate agreements. Make sure that we are educating and not falling for phishing scams. We want to make sure that we keep that information, that concept at top of mind and just reinforce the privilege that while we are working within the high level of data exchanges and concepts and technology that there really is a human factor and we need to remember that we are very privileged to have access to all this information. We need to be sensitive to that and do our best to keep it confidential. Thank you.

Melissa Goldstein: Thanks so much to you all. It is such a wealth of information and we really appreciate it especially from such disparate sources.

We will open it up for questions now from the panelists. I do not see any right now so I will start us off actually. This is a question for all of the people on the panel actually. Specifically, do any of the principles or policies or the technology that we have been talking about this technology and ethics panel differ in the context of the public health emergency so the emergency now and emergency in the future versus what we normally do day to day? Professor Allen, I know you talked about your principles not applying right now to this pandemic, but for instance, possibly to legislation that is

passed in the future. I am wondering about all of you. Is this only public health emergency what we have been talking about or is it all the time?

Danielle Allen: Maybe I will just jump in quickly on that to make sure I clarify. I did not mean to suggest that the principles I was articulating do not apply generally. I think they do. I think the principles that we are sort of articulating in a relationship to the exposure notification systems are concordant with the principles in HIPAA and aim for the same balancing of privacy protection and public interest. I meant at a level of infrastructural build out. I did not think that we needed to worry particularly intensively about exposure notification systems at this moment in time.

I do think though that we need to worry about integrating the rapid increase in volume of screening testing into our HIPAA protocols. But I was thinking as I watched everybody else's presentation that in each case, for example, the wonderful chart that – I am sorry. I have lost track. The commissioner from Tennessee, I believe, has presented, which had the four corners, public health, and hospitals and so forth. It was not really clear where some of the people who are providing the screening testing fit in to that; yet, they need to be integrated into our data system and they need to be folded into the HIPAA structures.

I think the principles we have or the principles we need even in an emergency and the question is in some sense more one of an organizational one. As practices change, can we adjust our structures to fold in new practitioners?

Kate Goodin: This is Kate. I would also just reply back and say that I also think that most of what I talked about is really a day-to-day issue that health departments are struggling with, this balance between data protection and personal privacy and where does that balance then tip towards a more public need for information in order to take those public health actions.

I think that the things about our current situation and about large-scale public health emergencies like pandemics is – does that line move between personal privacy and then public good or public need and how much time do you actually have to weigh those options because typically the scale of the response, the tempo of the response is different in large-scale emergencies versus your day to day like the example I was giving with food-borne outbreaks and that sort of thing? I think the principles again are reusable and are similar, but I think the scale kind

of might determine how quickly you need to make a different decision and where that line is between those two competing priorities.

From a technology standpoint, I would say that we would love for ELR and ECR to be more widely adopted because it is a simple technology that would allow day-to-day operations to work more effectively and to be scalable in these larger type of situations.

Melissa Goldstein: Thank you. That line moving and where it moves to is one of the things that we have talked about a lot. We are very interested in that.

John Loonsk: Thank you. Generally, I do believe that policies should drive technology. But an important ongoing public health consideration has been dual use and the term has real meaning from a technical implementation standpoint that one never wants to be implementing new technologies during an emergency. If you think about it from that perspective, it is important that the policies are also accommodating of how routine activities flow, how the data flow during routine and emergent so that there is not this need to scramble during an emergency to set up new data flows or new even policies for carrying them out.

Melissa Goldstein: Could I just ask one follow-up question to that? I am not sure you were with us for the first panel where we talked more – we were talking about mobile apps and the proliferation of the mobile apps. I wonder. Do you include the mobile apps in that technology during the emergency piece?

John Loonsk: I am sorry, I did not partake in that particular part of the session, but I think it is a general principle that I am trying to apply. I would presume until proven otherwise that dual use principles should be considered in advance because that is what enables emergency activities to occur seamlessly.

Stacey Katz: Melissa, there already exists in the State of Maine levels of use. HIPAA already permits the flow of information from the provider to – or from the lab to the provider and from the provider to the public health entity. However, in light of the public health emergency and there is sort of the extreme public health emergency so that certainly does broaden the ability and the public health entity, the CDC, the director to use and implement initiatives in order to quarantine and in order to contain the outbreak and that is a very flexible standard. What does it mean to contain and how broadly can we

use that – but it is necessary and the director has that authority?

Melissa Goldstein: Did you have similar exceptions in the Maine law?

Stacey Katz: Yes, we did. That is the Maine rule. There is basically the statute and then there are rules under the statute that sort of set out. In the case of an extreme public health emergency, our governor has declared, or the director has declared it. And it really broadens. It basically allows for containment of the outbreak within the context of a certain book. Basically, the definition basically says do what you need to to contain the outbreak.

Melissa Goldstein: Yes, okay. Thank you. Thank you, all. Denise Love.

Denise Love: Thank you for the presentations and also for the work you are doing to keep us healthier as a population. I have a question that probably is more directed to John and/or Kate, but anyone could answer.

I know a little bit about the CDC modernization efforts and the funding. Will this move the needle a little bit to give us the enduring infrastructure building we need for future pandemics?

John Loonsk: That is a great question, Denise. It is certainly a lesson I have learned having gone through many an emergency over the last couple of decades that that is when the funding flows. That is when the tension to public health is in place and that is when you can move the needle on public health.

That being said, a lot of technical implementation requires sustained funding and that has become very problematic in public health over the last decade as the sustained funding for public health and particularly public health IT has dwindled.

The data modernization money started at $40 million level. Obviously, they moved to another order of magnitude in the context of the COVID emergency. It is critical to think about how those can be implemented such that they can be sustained over time because this is the opportunity. As paradoxical as it is, this is – the hardest time to move forward is also the best time to move forward. We have to make it work.

Kate Goodin: I would definitely agree. I think that the data modernization money was coming to state and local health

departments right as some of the COVID funding announcements also came out. It was a little bit of a timing challenge as Dr. Loonsk said of how do you start implementing data modernization pieces while trying to accommodate the current level of necessary communicable disease response.

I am ever hopeful that it is going to be very impactful. I think that it has been echoed and reinforced through several of the COVID funding mechanisms where things like ELR and ECR are emphasized as activities.

I think that some of the challenge that we face in public health is as much as we need our infrastructure modernized and as much emphasis as there has been in the public sector or the private sector among health care providers for EHR implementation and meaningful use, the level of technology interoperability is not necessarily there on either side and we still have technological challenges, having large health care systems create these HL7 messages that have been established again as standards for many years.

There still seems to be a disconnect between how some industries view their interaction with public health as a priority, meaning that they do not typically see it as a priority. It has led to a de-emphasis of spending resources on interoperability with public health.

Melissa Goldstein: Thank you. Vickie Mays.

Vickie Mays: I want to thank all our presenters for some really insightful comments that they have made.

I want to direct my questions to Professor Allen. What you are presenting I am greatly concerned about. It is great that you have highlighted these issues and that is this issue of testing and who owns this testing in certain settings because it is not being seen as part of HIPAA. If you have this experience – at a major university. We have our own academic medical center and they are going to do all the testing and processing of testing. We have been asked to do everything from – if we are COVID infected to call a hotline and just leave the information there. We are told that our test data has to be sent to the university. It is just an incredible – reach. And the reach is occurring because of how people view their responsibilities, but also how people will view the ownership of some of this data – not being collected in a really –

I am wondering if you could speak very specifically to what is the how. You say you need clarification – HIPAA applies to screening testing sites. But what is the how to move the needle? What is the policy that is needed to bring all this under the umbrella?

I think my second question is the tests are being owned by such different entities that the tests are not necessarily all equal in quality. Do you think they also need to have a standard set with these tests?

Danielle Allen: I think a lot of people are working on this right now. I think there are a few components. I think of the first instance. We do need CDC and HHS to align vocabulary and categories. We need a common vocabulary, which we do not have. We are struggling with the fact that for this screening testing, individuals are returned – results are returned to individuals. That seems to set it apart from traditional public health, which is working in aggregate data and anonymized data.

In that regard, it feels like it is not surveillance. It is something different; yet, it is fundamentally a public health function, this screening activity. We really need to go ahead and name the category and then work through our regulatory structure and I would say starting with working – public health regulatory structure to figure out where we need adjustments to make that work. I think this is the job of HHS and CDC. I do think it is time for a rules adjustment around HIPAA that expands the category of covered entities because it is not adequate to the activities that we are currently seeing. I think that would be a first and really important point.

And then I think once we actually have a clear category that we could name, then, yes, we can do the work of standard setting. There are civil society entities that are trying to do this. For example, the Rockefeller Foundation that came up earlier around the testing data commons idea. They are also trying to establish a framework for how different categories of screening test, what role they have, what is their appropriate use for them and so forth. At the end of the day in an ideal situation, this would not be done by civil society organization. It really would be done by the HHS and CDC. I am sure I am speaking to the choice in many ways on that point. We need that common vocabulary. We need that clarification around core categories and to recognize that.

We have quite a voluminous body of activity now that falls between the two stools of the categories we are used to using and we need to address that.

Vickie Mays: Thank you.

Melissa Goldstein: Thank you. Denise Chrysler.

Denise Chrysler: Thank you everybody for your insight comments. As we know, public health is sort of between a rock and a hard place. It is walking a tightrope, trying to protect privacy, yet, needing to keep the public informed. Trust does not only mean privacy, but trust because of transparency and sharing information with the public that is disaggregated enough so that you could see disparate impact on individuals say from COVID-19.

And if you look at like HIPAA standards, they will not even allow you to share employers for individuals who are affected by COVID or a lot of demographic temporal and other disaggregated information.

Have you experienced, and this is especially for our two public health practitioners, times when either law or policy has prevented you during COVID-19 in sharing information that really would be important to share with the public, to share with grassroots organizations, to share with others that may be empowered to use the information in ways to address disparities?

Kate Goodin: I can kick us off on that. I would say that one of the challenges we have faced, which is not directly in answer to your question, is the lack of some of the data that would allow us to do that type of disclosure so especially things around race/ethnicity, gender, gender identity. We are just not getting that data in the completeness that it needs to be in order to make some of these conclusions or action steps around specifically affected populations. That has definitely limited us from a content perspective.

I think to go towards your actual question around what if anything have we been limited in doing, I would say that in Tennessee specifically, some of our initial reports and disclosures to the public were poorly received by some populations. It led to kind of a large step back. Rather than kind of going slower earlier, we went a little quickly earlier and then needed to reassess where we were at as far as what data was being published, what information was available, to which entities and which organizations. It kind of made us really go back and rethink what was being provided in a way that probably

did stop us from disclosing more information in a more timely way because we had some of those negative reactions early on.

I would also share that occasionally some of the challenges in this particular response have also been related to how the data is perceived and interpreted by any reader. There are obviously limitations to how much annotation you can provide in a report or a data set, how much meta-data you can provide around the records you are disclosing. You cannot provide every piece of context that would happen if you yourself writing a report say or a fact sheet as opposed to just allowing a data set to be publicly accessed.

There has been a lot of time and work taken up by needing to explain data again, explain categories again, explain categorizations again, that sort of thing that has maybe I want to say disincentivized because people are still releasing data as appropriate, but has led to some additional work associated with data disclosures of explaining what it truly means, explaining how to interpret different fields that cannot adequately be captured in standard documentation, footnotes and meta-data.

I would say the other piece of impact to public health agencies around data disclosure has been additional analyses completed by outside groups, interested parties, that sort of thing, which is what data sets are intended to do, but have led to some maybe again not totally erroneous but perhaps not fully explained conclusions around that data, which then take a lot of public health agency time to reexplain like what the data analysis should have taken into account or what it did not factor in and that sort of thing that affected their conclusions. There is a lot of time taken up with messaging, with rumor control, with that type of thing associated with these disclosures, which is taking up a lot of public health time.

Stacey Katz: I just want to jump in quickly and say, yes, a lot has to do with education. In answer to your question, have we ever held back certain information perhaps that folks out in the public wanted and the answer is yes. I think that part of this comes with educating the public and the listener. Dr. Shah, who is also an attorney as well as a physician, would explain that. No, you cannot find out who is on your street who you think tested positively even though you think you are entitled to that for your public health purposes. Here is what the law is around public health, privacy, or independent privacy versus – you will know that it --

Melissa Goldstein: Professor Allen, Dr. Loonsk, do you want to add anything?

(Nods no)

Melissa Goldstein: We will give the last question to our subcommittee chair. Frank, go ahead.

Frank Pasquale: I just had this one last question. I know we are short on time and so feel free not to – or a later comment. My one question would be if there are any particular rules or practices that you believe are impeding response, public health response that we would be aware of them because I think that there is a real issue in terms of I just sometimes find myself between the poles of two very different points of view on this matter, one of which is giving me a sense that there is a bramble of rules that is just really impeding the ability to make data as usable as it can be and the other being sort of reports – other places saying that privacy is sort of under protected and there is an under protection of privacy and there is so much information out there about people.

My question is just if there are particular rules or standards or practices that you find troubling either to isolate them now or in after follow up because I think it is a really difficult question that would be helpful to us to understand.

Kate Goodin: I guess just really quickly I would say that one of the biggest challenges is not a particular law or rule, but more generally the patchwork of rules and laws that exist across states and jurisdictions so locally defined rules could be in conflict with national standards or national laws or federal laws. There is definitely that risk, which could make implementation of a national standard difficult within a state or a local jurisdiction.

I would also say – this one has not been mentioned today and it has not been such a challenge in COVID but has been a challenge in past responses and that is FERPA. Educational law has significantly impacted communicable disease control. When children within a school environment are exposed to a communicable disease, identifying who is in the same classroom, identifying who has afterschool activities together has not been possible in many situations because schools feel that they are not able to disclose that to public health entities.

Danielle Allen: I would second the point about the patchwork. I think that is the fundamental issue. I think we are all crying

out for a shared strategy for approaching data and that is partly about categories and meta-data and everything that we were hearing about today. I think that is the issue rather than a specific rule or regulation and both makes some places leaky because of confusion and it makes other places sort of focused on providing the data that is not necessarily the most useful. It is really the lack of coordination I think that is the challenge.

John Loonsk: To the comments on patchwork, I would add understanding, understanding what – enable to get, working directly with clinical care, which we are doing more than ever before, convincing compliance officers that actually public health is eligible to get data is not a small task. That component is something else that could use attention.

Melissa Goldstein: Thank you, all. This has been a spectacular panel and thank you all so much for joining us today and for sharing your time.

Rebecca, I think now we have a break for 15 minutes before the third panel.

Rebecca Hines: That is the plan. See you all in 15. Thanks again to our guests. Very grateful for your time and your expertise.

(Break)

Panel III – Bias and Discrimination

Denise Love: Welcome back, to those of you who have joined us after the break, and this is the third panel, a very important one that sort of caps our hugely robust discussion that we've had throughout the day, and one that promises to be quite interesting in how we put it all together.

The way I see it is COVID has accentuated the existing deficiencies, in not only society but our data ecosystem, and how we go forward will be critical and all the lessons learned. So I'm just so pleased to introduce this fine panel.

I'll read their names and titles, but I'll remind you again the bios are on the website so you can do a deeper dive.

First we'll hear from Bryant Thomas Karras. Dr. Bryant Thomas Karras, Chief Informatics Officer, Office of the State Officer/Chief Science Officer, Washington State Department of

Health. We'll then have Dr. Mary Gray, Senior Principal Researcher, Microsoft Research, as a second panelist.

The third will be Dr. Sean Martin McDonald, Senior Fellow, Centre for International Governance Innovation in Ontario, Canada. He is a lawyer and CEO of FrontlineSMS, as his short title. And then we will have Dr. Wang, the Director of Center for Policy, Outcomes and Prevention at Stanford University.

What we'll do is start with Dr. Karras first, and then run through the panelists as read.

Bryant Thomas Karras: I want to thank the committee for allowing me to speak today, and I want to also thank the previous session, colleagues of mine, John and Kate and Stacey did a fabulous job in sharing their perspectives, so it makes my job easier in pulling it all together.

I first wanted to start with an acknowledgement. I'm broadcasting from the ancestral lands of the Duwamish people, whose land was taken from them under duress in the Treaty of Point Elliott in 1855, to pay respect to their elders, past and present. Past elders included Chief Seattle, the namesake of the city that I live in. So I want to take a moment to acknowledge the past, the many legacies of violence, displacement, migration, and settlement that have harmed indigenous people across this country, and think about the folks in the communities where you live.

Quick overview of some of the things I'll cover. Several of the topics were covered in detail in the morning session and the previous session. I may skip over some things quickly to get to some additional topics.

I think Kate in the previous session did a great job of describing contact tracing, case investigations, and in the morning session there was a discussion on how exposure notification fits into this, so there's a good framework, but I wanted to share this infographic that we have publicly posted on the Department of Health website to help convey what's going on in this situation, and the fact that this is not a new process that's being introduced, but it has been around for quite some time, and it's really the bread and butter of the work that we do in public health.

Part of what we need to emphasize, I think, it's a focus of this committee, is that what case investigation/contact tracing is not. It will never ask people for their social security

numbers. In Washington State we never ask for people's immigration status or any financial information. Not even marital status or any other governmental IDs in terms of linkages. It's critical that, and I think Kate mentioned the unprecedented scale at which people are not participating in contact tracing and case investigation. We really need to start thinking of new solutions and new tools to be effective in regaining public trust.

So I'm going to go back in time. Some of you may remember that Washington State was the location of the first incident case of COVID-19 in the United States, so we've been at this for a while. Our incident command ramped up in January, and at that time we had our system for responding to cases was our laboratory information system that we call WELRS -- Washington Electronic Lab Reporting System -- would receive electronic laboratory data from all the lab submitters that are required to report to Washington State Department of Health on behalf of local health jurisdictions. And then we would put those into our case management system, which we call Washington State Disease Reporting System. It's a commercial product known as MAVEN that's used in many other states as well.

Very quickly, in the course of this pandemic, this unprecedented outbreak, we realized that MAVEN, in terms of scaling it up to meet the needs of the volume of cases, and the electronic system that we were using to collect laboratory data, was being overwhelmed.

So we migrated, we accelerated a project that we had in the queue to migrate these systems to the cloud. It was actually funded through HITECH and CMS's 90/10 program, migrating our lab system and our WDRS system to the cloud, and adding in a new tool, REDCap, to speed up the interviewing process.

Then as the epidemic, pandemic, continued to expand, we projected out that the -- even placed in the cloud environment, the REDCap system was not going to properly scale up to the number of end users, contact tracers and case investigators that needed to be using it simultaneously. So we quickly migrated yet again to another system, which is a Microsoft product called ARIAS, built on the Microsoft Dynamics PowerApps platform.

In addition, there were a lot of other systems outside of our agency. The circles in purple that were needing to interface with our work, as well as systems inside our agency that we needed to interoperably connect with our processes. So a lot was going on. In addition, thanks to MITRE and CDC funding, the

SARA Alert system was stood up. You heard about that in the previous session from Kate, as well, and that was used for symptom monitoring of these cases and contacts.

So a lot of new systems brought up in a relatively short amount of time, and a tremendous work and I'm really proud of how our agency was able to put in the many hours of work to accomplish these transitions.

There's way too much to talk about here, but I just want to highlight some of the challenges on this increasing complexity, needs, workforce with expertise to implement and utilize it. We recognized early on the need to for that extensible cloud-based capacity in order to scale up and meet these needs. And the integration of multiple data sources poses challenges, in time and making sure that it's done carefully and effectively. There were several time periods where we had some reporting delays because of migrations and changes that we needed to make to our systems. But they all were able to successfully resolve through the diligent effort of the management team.

I think in the last session Professor Allen talked about laboratory reporting, and I think accurate demographics and accurate actual address and telephone information on folks who are receiving new tests, proved to be a huge barrier in our successful response, and I think this underlines the need for a master person index, some better way to identify people, especially -- laboratory reports would come in with only partially complete information on cases. Lastly, the need for protecting privacy during the reporting, public disclosure requests, and dashboards need to make sure and take privacy very seriously.

The next slide is an example of our dashboard that we quickly stood up with volunteer support from Microsoft, and have been able to dynamically, every day, show what's happened in the previous 24 hours.

There's a whole ton of things that I could talk about, but I only have about five minutes left, so I'm going to jump right to one that I think is the most novel, most critical, and probably of a great deal of interest to your committee, the Bluetooth Google Apple Exposure Notification technology. The other technologies here that are highlighted on the integration slide that I showed, as well as what's coming down the pike in terms of the need for MPI and better laboratory data, are equally as important and are a foundation that's needed in order to add an enhancement like Bluetooth Exposure Notification.

Here's the use case. This is not photoshopped or staged; this is, if any of you, like myself, ride public transport, you know that everybody spends the entire bus ride on their phone, and that's a reality across the sociodemographic spectrum. It's critical that we are able to determine those people who have been in close proximity, especially those who were not abiding by rules of wearing their mask, so that if somebody becomes positive we can notify all of their close-proximity persons around them.

You heard in the first session about the exposure notification technology. We have been partnering with Apple and Google for quite some time. In an unprecedented effort, these two companies offered to stage this shared technology platform to support our public health work, and our experience in Washington State is that both organizations were extremely interested and receptive to hearing about our public health needs and requirements, and Washington is currently making deliberate choices to only consider apps and technologies that are voluntary and which preserve privacy and trust.

And I'm going to state that while we have not yet made the final decision about implementing activities, as of last week we are still actively exploring the Apple Google platform that appear to meet these requirements, and the University of Washington is working to pilot this technology on their campus.

I'm not going to read this slide to you, but this API does eliminate a lot of the concerns that had been seen, and there's a lot of perhaps theoretical or misinformation that has been shared by the press. I can tell you, we have done a deep dive and the technology itself that is one of the most promising things I've seen in my career, and I was one of the forerunners of syndromic surveillance, which was, I thought, a career-changing technology, and I think this may show to be another game-changing approach to public health needs in this age.

I'm running short on time, but I wanted to not read to you these slides but offer them into the record. We do see tremendous privacy concerns in some of the activities that are happening at the federal level, and we want to make sure that we take the privacy and confidentiality of our citizens in Washington State very seriously, and are doing everything we can to ensure that folks' identities in reports that are deidentified and sent to the CDC are not in some way reidentified.

This of course is in a balance, we heard in some of the previous sessions, with the ability to offer up research datasets,

compared to the ability to maintain people's privacy, and we need to make sure that everything is done to ensure that things are done in a proper way.

Skip past this, this is our small numbers policy.

And I offer a preview where we're going to be submitting in the next 24 hours some comments from our Secretary of Health.

I'm going to offer some final thoughts. I think there are some standards and coordination that's lacking. Several of the systems that we've heard about and that your committee is interested in are operating on the fly, and as we say in public health, some of these things are connected with spreadsheets and duct tape, and we really need interoperable standards to make these connections much more successful and automated.

I think that several of the case and contact tracing systems that states have stood up in recent months are fabulous enterprise-grade systems, but we need effort and assistance from HHS to ensure that these systems are not built in proprietary ways that public health can't use interoperably with neighboring states.

SARA Alert, which is a system which is in use in many states, is utilizing interoperable standards, but it can't be a one-way street. If they have the APIs to do this interoperability but the systems we need to connect them to don't, then we've missed an opportunity. Bluetooth Exposure Notification, as well, has a tremendous opportunity, but it's become a matter of state self-organizing, and we really need for this to be a success story. We really need it to be a successful adoption.

Care coordination is a topic that I'm not going to touch on today, but I think it's something that needs addressing as well.

I'll finish with a thank you to all of the diligent public health employees in my agency who have been part of this response. We've finally have backed off from 12-hour workdays to a 11-hour workdays, and gotten some of our weekends back as the pandemic has subsided a little bit. We imagine that -- we're staying diligent, and we'll see if projections bear to be true. This workforce is critical, and the folks who have been most valuable to us are ones that have gone through proper training in public health informatics, and the most valuable workforce members actually went through a program called the public health informatics fellowship program, that was sponsored by the CDC.

Unfortunately, they were incredibly overworked because of their expertise, that they alone had, and several of them have resigned now just out of pure exhaustion, needing to move on to something else. Unfortunately, the CDC has not been funding that program for the last several years, so there's no one to come back to recruit and fill their bed.

This is the last one, just the number of hours going all the way back to January. This is not cumulative, this is per month, it has increased. I just want to thank everybody for their efforts.

Thank you so much.

Denise Love: Thank you. The workload graphic there is quite astounding, and my hat off to everybody who's been working overtime to keep your citizens safe.

We'll move right on to the next speaker, which is Dr. Gray. I want a do-over on her introduction. Dr. Gray is a Senior Principal Researcher at Microsoft Research and a fellow at Harvard University's Berkman Klein Center For Internet and Society, and I'll turn it right over to you, Dr. Gray.

Mary Gray: Thank you. Thanks for the opportunity to address the committee today. I wanted to start with an appreciation for Professor Pasquale's opening remarks about the importance of seeing the need for health data stewardship as a north star for this committee's efforts.

While stewardship, it's critical, we also need to approach this pandemic as an opportunity to build the ongoing partnerships with communities that will be critical to not only contending with COVID but to the work of rebuilding and tending public health in the aftermath of the pandemic, and several panelists have noted this need for building the public's trust, that in many ways the breach, the lack of trust, is making things so much harder.

So I have three interconnected points that I'd like to make with the time I have allotted. The first is off-the-shelf mainstream security and privacy techniques that I've heard referenced kind of generically throughout the day, that deidentify data to protect patients' identities, are very limited. Failure to recognize this means that public-private partnerships that are collecting individuals' data cannot be the good data stewards and community partners that we need for the data collected. I can't say that enough.

The overreliance on deidentification alone and the trafficking in largescale data without the public's buy-in, arguably without their understanding, is risking further erosion of the public's trust, and we can't afford this in the second and third wave of this pandemic or future pandemics. So that's the thing. We're playing with fire, quite literally, in thinking about collecting data now as though it's going to be useful without this awareness of the limits of that approach.

Then the second point I want to make is recognizing that we cannot guarantee people's privacy when we collect their data. We need public health approaches that focus on building trust with communities that are disproportionately absorbing the impact of COVID-19, and we haven't really been seeing much effort, to be quite explicit, about the need to recognize who's being hardest hit. The question is how to do this effectively, perhaps, and to date, our technological solutions have focused on individual privacy and security, ignoring the need to build individual and community trust through our technologies.

And the third point I want to make is toward that end, of building individual and community trust, aligning but hopefully building on several of the presentations today, my comments are going to focus on a call for government agencies to come to grips with the limits of deidentifying public health surveillance data, as well as the limits of generating meaningful data from individuals who are anonymously sharing it through digital contact tracing or proximity notification technologies. While they seem really hopeful, and we keep pointing to other countries that have success with these technologies, we have to come back to the basic reality that every country where these technologies have been marginally or reasonably successful, there's been a really robust public infrastructure in place. We do not have that.

So instead, based on preliminary studies of Pandemic Response Network, a community-centered approach to patient monitoring and support out of Duke Health, I'm advocating for public health departments to pivot to training and equipping and partnering with -- deputizing might be the way I would put this -- key community groups who could serve as boots on the ground among those that are higher risk of exposure through occupation and vulnerability through comorbidity.

So let me start with my first point about deidentification. My day-to-day is with computer scientists and engineers, and they would be the first to confess that it's widely known, since 2000, when Dr. Latanya Sweeney, now at Harvard, published her

results, that you can identify 87 percent of the U.S. population with just a few identifiers, and about half of the U.S. population is likely be identified with just place, gender, and date of birth. You can buy that on the internet today from just about anybody on this committee call. I can find out all of that information, paying almost nothing. So the problem isn't the dataset that you might collect. It's that it can be assembled, it can be enhanced with other datasets you can purpose, that make anybody we're collecting data from easily identifiable down the road.

So really taking to heart that deidentification is not anything more than a moment of capture. It does not secure or keep anybody's information private. That's why the 2020 Census switched to differential privacy to protect individual respondent level data. It's not an effective means of protecting people's information. Really absorbing that reality, not hanging our hats on deidentification. I want to note, as Denise Love noted earlier today, that most of our regulations and practices around collecting and protecting patients' data are more than 30 years old at this point and do not grapple with this reality about deidentification, that it's literally a moment in time. It doesn't protect anything in perpetuity.

While our capacity to use data science for modeling disease and public health have absolutely advanced, our mechanisms for meaningfully engaging the public and getting people's consent and buy-in to learn from their data are failing us. This perhaps helps us understand why, as Kate Goodin noted in her presentation, why so many people hang up when they're called by a public healthcare worker. People don't trust what's going to happen next, and we are easily contributing to that problem right now, by collecting data and having no awareness of what limits there are to that data collection and what vulnerabilities we might be introducing.

So given the ongoing sense of urgency, some particularly in my world and tech sectors are wondering if we should really be waiting for a healthcare worker to call someone to track down the virus. But in a fight that depends on quickly finding and containing the virus, couldn't we use mobile phone data as other countries have used it? All of these different datasets that already connect us, and trace our every step.

Unfortunately, this line of thinking has dominated much of the debate about how best to apply technology particularly in contact tracing, which I believe as somebody earlier noted, there's such a misunderstanding of what that involves. In many

ways, the phrase contact tracing really elides the harder more important work of creating an ongoing conversation between healthcare workers and individuals who may, at a later date, contract COVID. So identifying and tracing potentially affected people are really just the first steps in this process. How would we create technologies that assume we're going to be calling somebody back?

The frontline human contact tracers need to persuade people, particularly those at community's margins, whether we're talking about working with undocumented folks or the elderly living alone, are the ones who need our support. We need to build technologies for those workers. Much of the work of stopping COVID is going to involve equipping communities hardest-hit and those healthcare workers tending to them to quickly muster resources to monitor and manage patients' health, rather than just identifying who might have been exposed and assuming that that data modeling helps us intervene.

Contact tracing is really the core element of all of the plans that we've needed to put in place for safely easing social distancing and shutdowns that are the result of the pandemic. It's been around -- I don't need to tell this committee -- for over a century. It is the proven standard for managing life-threatening infectious diseases. It allows us to systematically map who's been exposed, but it does that by maintaining some sense of ability to go back to people who've been exposed and find out the networks with whom they might be interacting to advance that exposure.

In other words, the success depends both on meticulous data collection, but also on being able to effectively counsel people to talk about their exposure risks. No one receiving a text message about being exposed to something that might have killed their aunt is really in the best position to just on their own respond to such a notification. It really takes somebody caring, who quite literally speaks their language, to be able to draw out the information that we might need to understand who else has been exposed and how to take care of someone who needs to self-isolate in that moment.

So that's why a successfully contact tracing really requires counseling skills of trained healthcare workers who are connected to the communities that they serve. This is the piece we're missing. The magnitude of the labor force needed for contact tracing absolutely feels daunting, in some ways because we're treating it as though it's something that's going to happen by large mobilizations of a national army, instead of

thinking very locally about the clusters of outbreaks that we've had and who might be best positioned to be able to tend to the communities who are hardest hit.

I want to speed through some of my comments just to save time. In many ways, the turn to digital contact tracing forgets that we need this broker, you could say, this deputized extension of public health, and I want to talk about why digital contact tracing apps and proximity notification and exposure notification apps, which, frankly, are just phrases and terminology that keep shifting as there's an effort to get the public to be interested in downloading an app that might monitor their movement and their interactions, that often the cellphone data will miss, for example, data from an infected person who leaves their cell phone behind while they go grocery shopping. It will miss the millions of people who don't have their own cellphone, who live in rural parts of the country with limited cellphone or cellular internet access. And most crucially, learning this from the Pandemic Response Network, it's going to lead to inaccurately reporting the nature of such contacts.

High-risk contacts range from being within 6 feet of an infected person who's not wearing a mask for longer than 10 minutes to touching a contaminated surface. We're still learning so much about COVID that we don't fully understand what are the exposure risks, depending on your relationship, your proximity to someone. So as mentioned earlier, the positive, the false positives and false negatives likely to generate from an exposure notification app just isolated from somebody counseling through looking at your history of movement, are astronomical. They would create such a burden for trying to go through the material that's collected from the data collected.

To be successful, any of the data collected is going to need to rely on trained healthcare workers able to assess the potential risk associated with each interaction. And this in turn is going to require the ability to patiently encourage someone who is sick, or potentially anxious about being sick, to remember who they interacted with, under what relevant conditions. That's just no small thing, and we've not done much to improve the equipment, the toolkit, for these health workers who will do that work.

But I would argue, most problematic is assuming that the nuances of contact tracing can be reduced to simply tracing networks of contacts from location data. We're putting a lot of trust in location data as a panacea for what is arguably a problem of people being able to relate their interactions with folks, if

they don't feel comfortable talking about who they're interacting with.

Specifically, I'm thinking of undocumented workers in settings, and I'm thinking about people in work settings where they're going to avoid communicating their risk exposure so that they don't lose their jobs. In any environment where somebody isn't fully consenting or in an environment where an employer hands them an app and says please use this app to monitor your health, odds are pretty good that that's coercive. Most cases, we would never allow consent to count within a research setting if we know that there's any sort of relationship, a power dynamic, that would leave somebody feeling that they can't say no.

Why does that matter? Because we know that in most cases, those who are most vulnerable who have a reason not to trust who they're communicating with about their health status, are likely to misrepresent where they've been and what they've been doing if they feel that it's going to put them at greater risk of losing their job or losing their livelihood in some other way.

So we're forgetting that the folks who are most vulnerable are precisely the ones who need to trust the people they're talking with the most. That means contact tracing hinges on these deeply human exchanges that are all about trust, not privacy and security or anonymity.

To narrow focus on cellphone location data is distracting policymakers, is distracting all of us, frankly, from building out the ranks of community-based workers, healthcare workers who could implement a comprehensive contact tracing strategy with mechanisms for holding people's data in trust, and I'm looking forward to the conversations about data trusts and the conversations about data commons that we've been having.

These monumental contact tracing efforts are going to require technologies that are literally built to assist these community-based contact health workers, and contact tracers, for not just the months in which we're leading up to vaccines, and in many ways, to be part of the loop of helping people get vaccinated. This can't just be about identifying the location of diseases.

The kinds of technologies and the kinds of data sharing that we need, the recommendations that I'd offer, they have to be intentionally built to assist rather than attempt to replace the vital piece of contact tracing, the caregiver in the healthcare loop. We haven't had much conversation about equipping that healthcare worker to share data with others. The tech design

for helping healthcare workers to coordinate care for family and friends in the midst of the aftermath of the virus are going to win the day.

So let me offer a few suggestions that are drawn from computer science and engineering to point toward more collaborative work technologies and data sharing that might be of use in this moment. First of all, we need dynamical electronic reference tools that are going to provide well-indexed access to answers likely to challenging questions that individuals are going to have, and they have to, again, be literally written in the language of the person who's seeking information about their health status. To date, there are many cases in which states don't even have access to any screener language for healthcare worker in anything other than English. That makes no sense in this country. So there are just some basic places where you can't possibly collect the data you need because we're not even speaking the language of the person who's trying to share information about their health status.

And for the long-term monitoring of people's health, we're going to have to be able to assist teams in sharing information about where people have been quarantined and how we would route resources to them. What kind of support we can offer from getting groceries for someone to taking care of their childcare needs? Those are all going to require information sharing rather than the kind of security- and privacy-first approaches that are quite individualistic right now, in the way we talk about them, and that for the most part have been outside of the debate about how do we deal with our current crisis.

Lastly, healthcare community workers and their agencies across these private/public partnerships are going to need secure centralized data storage. Again, the conversation around data commons is so critical, but I would argue we actually also need to be thinking first about building community data trusts. How would we be talking with individuals who are sharing information about their locations, about their health status, and let them know that we are going to enter that information into a data trust that a community can hold and that a person could literally be able to lock with particular informed consent in place from the beginning? And the community members could then be able to say who they would like that information shared with beyond the basics of positive and negative reports about health status.

Could we go to that fairly radical place of accepting that we need this kind of assumption of dual purpose for data for public

health surveillance upfront, and Commissioner Arwady had noted that the distinctions between data analyses for research and public health monitoring are often complicated. Another way of thinking about this is when it comes to data modeling and data science, the kind of resources we need for being able to understand the spread of this disease, there's very little distinction between a use for research and a use for application.

In my world this is called a A/B testing. The main technique for data modeling relies on a constant dipping in and out of live streams of data. So we should assume that people's collected data could always be ripe for repurposing and proceed with care in full enfranchisement of people to their right to participate in controlling data about them, that in the long run we're going to be better served from this approach, rather than assuming that we can take people's data, protect it for them, and leave them out of the conversation.

The last thing I want to note is that glamorizing this, the promise of tech and assuming it's going to substitute for healthcare workers who are going to be at the core of what we need to do, isn't just wasting time. It's costing us lives. Millions of Americans who don't have internet access, share smartphones, are the ones we're going to miss along the way, if we take an approach that assumes a proximity notification app will do it, or that if we start with places like schools or employers, who can manage their own community members' health, but imagine the rest of the public's health is somewhat irrelevant. It's circumventing the function of public health to let there be such a decentralized approach, and I think Denise is about to tell me I'm running out of time.

Denise Love: You have given us a lot to think about here, and I'm sorry, but we'll have to move on, and we'll come back and circle with the discussion if we have some time at the end. Thank you, Dr. Gray.

We're going to move right along to Sean Martin McDonald. I'll turn it over to you.

Sean McDonald: One of the benefits of being this late in the day is that a lot of the themes have been covered, which is great news, but I want to thank the committee for inviting me to comment. I think I was probably invited because I've been focusing on, or looking at, digital contact tracing since the Ebola epidemic in 2014. And what we found then, like Dr. Gray says, is that focusing on movement not only was a terrible for

proxy for actual disease tracking, but it ended up happening in the middle of the trust crisis, which significantly fueled the spread of disease. And, as it turns out, was illegal.

One of the things that we've talked about a lot here in terms of law and policy is when particular legal regimes apply. But of course, without affirmative emergency powers, we're not necessarily moving away from preexisting protections and limitations on state behavior.

The question is what has COVID, what has the most recent round taught us, since the Ebola epidemic, about not just contact tracing apps, which I think have been covered pretty well, but about developing public technology generally? This is a little-known reactionary publication you may have heard of called the Economist, and this is the way that they're introducing technology about COVID to the public. I think that one of the things that's really clear and one of the things I really want to make clear in my comments is that there are biases inherent in deploying public technology, and that those biases not only create or need to intervene at the top of the funnel. Right now we're talking about a lot of data protection and HIPAA, FERPA was mentioned in an earlier presentation, but there are also a number of laws that govern how we launch products, particularly health-adjacent products, and it's really worth being thoughtful not only about how do we consider the role of medical regulators and medical public health actors in participating in those validation processes, but also in the communication of those processes.

To the extent that we've heard about the success of contact-tracing apps, I really want to be clear that what most people are referring to is maybe the adoption. The single largest number of notifications that I believe has been publicly reported is in the hundreds, and that's from millions and millions of people, and that says nothing of the kinds of fidelity of notification. Dr. Gray also mentioned earlier on that we provide a lot of human infrastructure in the way that we talk to people about health, as a necessary human connection.

We also fundamentally connect contact tracing to care. Contact tracing is a care ingestion process. So it's extraordinary important to recognize that applications, even when adopted, that don't also provide that degree of care, have largely been pronounced by their own implementers to be marginally helpful, if at all. I believe Singapore said that they had one unique case that they had identified.

What we have at a fundamental level, like Dr. Gray is saying, and many others have said before, it's just so recent, is that there's a fundamental problem in evaluating the underlying science before it gets deployed as a foundational set of assumptions through this technology. Whether or not you are thinking about how well the technology works in the end, we're still not actually centering whether or not these applications meaningfully advance public health goals. We're still evaluating whether or not they can be deployed on different platforms, or what rate of adoption they get, or whether or not they have computational security problems.

I think that one of the things that we forget in talking about the conditions of deployment, for example, is that billions of phones can't use the Bluetooth protocol implicatory, and that's not only a problem from the confidence interval of the quality of the insights that it suggests, but it also suggests that if we're focusing on a public health implementation that excludes, and knows that it excludes, this many people, then how are we credibly professing a public or equitable health response?

So I just wanted to give one quick example of L.A., again a little-known place that has been very active in talking about its contact tracing app. Very early on, lawmakers raised concerns, and for those who are nerdy enough to enjoy the comic strip XKCD, you know a lot of the discussion about abuse of either COVID tracing apps has either been about its data or its security or its sort of computational approach to privacy, where, of course, in practice, it's usually much simpler modes of abuse that get exploited.

Here, we just see, for example, that L.A. has decided that instead of deploying its own contact-tracing app, it's going to repurpose a criminal surveillant-tracing app, which was so invasive that it was kicked out of the app store initially.

Not only do we have this set of concerns around the process of developing these apps in good faith, and ensuring that we are not doing the things like invoking the worst known actors in technology to be the face of our public health technology responses, but we also need to be able to, as I believe Ashkan said earlier in the day, we also need to be able to protect the integrity of the term and protect the integrity of the brand. In both of those cases, there are commercial actors and sovereign bad actors, the sort of quote-unquote good name of contact tracing has resulted in a whole bunch of very political, very commercially exploitative action that has undermined the trust and understandably the faith of a lot of populations who

we fundamentally need to adopt technologies if they're to be a meaningful part of an equitable public health response.

Then there's of course the problem that a lot of these are actively causing problems, that the technology themselves have bugs, have data architecture problems, have not only false positives, but false positives for people who may not be able to change their life. There is the presumption that people will be able to abide by stay-in-place orders or quarantine orders without the social support to do that.

This is the Edelman trust barometer in 2020, which Edelman I think has been trying to find new ways to describe a trust apocalypse for years. It just keeps going down and down. But this year was really fascinating, because it demonstrated across the board how the way that industries adopt technology also affects the way that they're trusted. In other words, there's a politics involved in the communication and rollout of these processes, and an earlier presenter, I believe Dr. Goodin, said that there are a number of real issues where people aren't even picking up, and we'd like to blame an app, or we'd like to blame a technology, but we also have lawmakers out there who are making it easier to ignore or delegitimize. I think that those problems are a top-of-the-pipeline problem.

In other words, when we develop these applications, we know that there are these structural issues in play. We're too far in the development and deployment of emergency technologies to pretend that they're not political. We know that they're political because they're about your exposure to public institutions, and as a number of people have started to say, what it means to be optional and what it means to have consent when you have what are called second-order-of-magnitude compelled adoption, when your employer, when your education provider, when your local law enforcement requires you to or responds to your behavior in a way that is based on your ability to present an app.

And that's happening not only here. Chile introduced the first immunity passport. Singapore are already said to, in India, all of these have started to see pickup and adoption. We should expect, as someone mentioned earlier, that insurance industries and professional risk mitigation are going to drive the adoption of apps like this, regardless of whether or not they have a meaningful effect on people's wellbeing.

So the question then becomes how do we get involved? Of course, the way that most people experience digital rights is through a terms of service agreement, which of course all of the folks

here I'm sure read terms of service agreements, but one of the things that was very clear is that when your public health response becomes a product that doesn't involve a human point of contact, you have these long chains of quasi-commercial, quasi-consumer support services, or as a law you might get passed between three or four different communities or companies before you're able to get a response, and that's a kind of change in the character of a public health response that we typically don't allow. In the United States, obviously, we don't let you yell fire in a movie theatre, let alone tell someone that they might have the world's largest and least controlled pandemic disease.

That distance, that distance between what it is that we're telling people and the support that we're giving them in context to do the things that we're asking of them is leading to a lack of legitimacy, and it's challenging the way that our institutions are engaging with the public.

I won't go through all of this, but maybe some of you all will have seen the Economist coverage, but I think that when we talk about the potential of technology we also have to acknowledge that in its current form it is delegitimizing a huge number of the institutions and industries it touches, and it's doing so largely because we're not doing the diligence up ahead.

There's been a lot of talk already about how we think about experimentation and how it is that we think about patients' rights. I just wanted to raise the Belmont report. One of the things that I'm sort or curious about and surprised about in this conversation is how little we've talked about common code, and how little we've talked about essentially that we recognize that there are all of these very experimental characteristics of these public health technology deployments, but we don't have the same level of sort of guidelines and guardrails and institutional validation checks that we would want before letting them go to scale. Of course, while a lot of these are not funded necessarily through government funding, and while the common code has grown up substantially, it is interesting to think about what it means for a government to use its emergency powers to participate in science infrastructure.

I think we've also seen in COVID that politics sometimes trumps the rights of the vulnerable, and that we see that the things that are leading to different parts of the vaccine pipeline are not always strictly the most promising science. So it's worth thinking about when the government, when a government, when a politics, starts to engage and exercise its powers for the

public good, how do we start approaching or considering the typical protections that we usually put on emergency powers? Those are things like regular review, time limitation, independent oversight, budgetary review.

What we fundamentally found, though, is that science is dialogical in a lot of instances, and while it is best done in empiricism, during emergency it is difficult to sort through the noise, and we need ways to engage with the politics. To Dr. Gray's and earlier participants' points, that means in a lot of instances that we need to recognize the differences between research settings and contexts from practice settings. That's not only about whether or not something passed an IRB or lives in a university lab. It is also fundamentally about the way that we architect accountability.

I wanted to raise both in recognizing the politics of a lot of this data architecture, but also in the process of technology deployment, that we are fundamentally talking about political decisions. And it is important to recognize, when we're bringing education to politics fights, or expertise to accountability fights. In addition to the kinds of things where we hold ourselves and the industry and public health holds itself to a very high standard, we also need to create clear points of ingress for people who have disputes, for people who need to be able to correct the system, resolve individual disputes and rule-based disputes.

It's worth recognizing that when we look at professional ethics infrastructure, we almost entirely implement it wholesale or import it wholesale from bioethics, and technology doesn't have many of these fundamental institutional and accountability infrastructure that would enable us to seamlessly import that same type of ethical approach.

Someone's mentioned data trust earlier. My exploration around Ebola led very directly to how do we build accountability mechanisms where people and institutions can participate as equals or at least build mutual accountability? And a data trust is for the most part, at least in the common law-abiding part of the world, the most common and used shared governance over public resources mechanism that is independent of a public institution.

So said really briefly, trusts are based in equity law, but typically now implemented in property law, and the idea here is that a grantor puts an asset or the rights around an asset, which might be data, but here it might also be healthcare

representation, into a trust, and that active granting gives a trustee the authority to manage those rights within a specific context or that property.

It's like thinking of a power of attorney, but perhaps over data or digital rights. There are a number of use cases where these are already being used, Johns Hopkins Healthcare Center, Johns Hopkins Medicine, excuse me, notably, but there are a number of motivations, so thinking about how you protect data integrity and research settings, how you provide the sustainability or the usability of data, how you provide for representation of under-regarded or often marginalized communities, and actually the Facebook's oversight and safety committee, as controversial it has been, is actually structured as a legal trust.

So rather than thinking of a trust either as a panacea or as nothing, it is an instrumentation and as a tool that we can use to start architecting accountability that align and flexibly -- that allow us to flexibility experiment with the kinds of governance and the kinds of practice and the kinds of development that might actually start to remediate some of our small t trust issues.

So I think that the one thing I want to wrap up with is that while these structures exist, we fundamentally have to cope with the political nature of the way that we architect data, not only in sharing but as mentioned, I believe, by Dr. Allen in the formation of indicators in the way that we define data structures and where we put it. Most of our governance is designed as devolution, but there's very little at the international level.

I just finished up a project working with the WHO on their data governance. There is very little ability to sort of compel or to even really proactively engage with the politics that goes around these data governance functions, and I think we're already starting to see in a lot of ways the international attention that that can cause. I think it's worth reminding ourselves that in federal setups, we've already talked about interoperability as an issue, we've already seen different states take different approaches to setting standards around health technology. We need to build the infrastructure to remediate some of these political disputes or to find a negotiated solution, and I think in a lot of ways, it will start with building stronger research, user protection, and validation infrastructure.

So these are the conclusions. I won't read them to you. But I will say that I think that the most important thing to recognize is that while certainly privacy and confidentiality and security is the focus of this commission, that all of those concepts when viewed in light of a public health response, where every aspect of a culture, a society, is engaged are necessarily holistic.

So it's worth thinking about the degree to which things like insecure environments or unvalidated products that are advanced with at governmental scale but the rights and necessary means of redress and remediation are, and again, to sort of just close with the thought that Ashkan raised earlier, the technology will only create a certain amount of information, and the success of most of any endeavor of any contact tracing or COVID response that you can call successful has largely been the government's willingness to act on that information and do so in a way that encourage the participation and trust of its people.

So when thinking about things like privacy and confidentiality and security, which are obviously and necessarily technical, I would also invite this committee to be thinking about the ways in which they're going to have to rely on a wide range of actors and actions to create truly effective public health responses.

Thank you very much.

Denise Love: Fascinating. So much to think about.

We will move on to our last panel presenter of this afternoon, Dr. Jason Wang, and then we will hopefully have some time, because I think some of my committee members may have some good questions before we go into the next session. So I'll turn it over to you, Dr. Wang.

C. Jason Wang: Thank you very much for inviting me. So today I'm going to talk a little bit about the experience from Taiwan and then extensions, relevance to the United States.

This is based on a paper that we published in JAMA in March of this year.

So just to remind you, so Taiwan is about 81 miles off the coast of China, and it is a democracy. Has 24 million people, and about a million actually works in China. So they go back and forth. So last year, approximately 2.7 million people from China also visited Taiwan. So when the COVID-19 outbreak started, it was actually in very close proximity to the site.

So Taiwan had the experience of dealing with SARS in 2003, where during SARS, 73 people died, and almost all the infections were transmitted in the hospital, and several hospitals were shut down. During that time, there were not a lot of sort of legal bases for quarantine individuals, and so many people who were quarantined actually ran away, because they thought they were being incarcerated.

Since that time, there has been many, many changes made to the Communicable Disease Control Act. So the legislations basically were amended over the last 17 years. Some of the changes include the government's ability to have protective equipment stockpiles in place in almost all the hospitals. They set up a central command center, the national health command center. The law also allows for regulation of gatherings, entry and exit of people, traffic, evacuation, travel restrictions, and provided penalties for violating home quarantine and isolation regulations, and also for hoarding resources, disseminating rumors, or fake news, and they could fine institutions for inappropriate behavior and also allows for tracking and management of people under infectious risk.

So the government also during a pandemic or epidemic has special powers to request sort of productions of PPEs, and to use the facilities for -- and also essential medications. So this has all been clearly stated in the Communicable Disease Control Act that were amended in the past 17 years. The government's special power goes away within a year after the central command is activated.

So I just wanted to show you what a command center looks like. This is actually modeled after the United States, this blueprint. There's the command office, there's the data center, there are conference rooms, there are situations rooms, there's the media room, there are several conferencing facilities where people actually -- it's like a bunker. So it's on the 7th floor of the CDC, and they could host 100 people, 24/7. So there are people there all the time.

So the data come from both sort of different government agencies and also local governments, in real time, and there are data analysts. So this includes the National Health Insurance stockpile system, the National Infectious Disease Statistics System, and the media surveillance system. Also, has data from the immigration and customs system.

So as early as December 31, Taiwan CDC was notified that there is a possible transmission of human-to-human transmission of

coronavirus. So basically they started to board the airplanes of people coming from Wuhan, and they activated the command center in January of this year. On January 21, they also, the government called a national security council meeting to coordinate activities between various government ministries and agencies.

On January 27, the National Health Insurance Administration and the immigration and customs database were basically merged where data were sent from the immigration and customs, the last 14 days, to the National Health Insurance database, and this was accomplished in one day.

So this is when they boarded the flights on December of last year.

So I'm actually physically in Taiwan right now, undergoing quarantine. So I just went through the process. When you enter the country, they ask you to fill an online declaration form of symptoms during the last 14 days, and also the location where you are coming from and the countries you have been in the last 14 days. Based on that information, they either give you a green pass where you could just go through customs or they ask you to do isolation, if you are coming from a high-risk country or if you have any symptoms. They send you directly to the quarantine facility. Now, if you get a green pass, then you get to quarantine at home. That's where I am right now.

So as I mentioned to you before, they linked the customs and immigration database with the National Health Insurance database.

So when the doctor or nurse is seeing a patient, he or she will be alerted that this person just came from abroad and has been travel to some of the high risk countries, and they will be wearing PPEs and order a COVID test if there are any respiratory symptoms. This is after 14 days of quarantine. So you cannot go directly to go see a doctor without going through the health department if you are within the 14-day quarantine period.

So I want to discuss a little bit about digital epidemiology as it's relevant to this discussion. So first I think when we think about digital epidemiology, we have to think about the core public health functions, which is case detection, contact tracing, isolation, and quarantine. So to the extent that we have our sort of toolset, we have to make sure that the response actually is sufficient to meet the challenges of the epidemic.

So in this case, COVID-19 transmits very quickly, and so if your public health system is really slow to respond, then it would just keep spreading. So they have no ability to do contact tracing, no ability to isolate and quarantine, basically you basically don't have a lot of tools in your toolbox. So the previous speaker, two speakers, mentioned trust and public participation are extremely important. So how do we engender trust and participation I think is a key challenge to any government and especially democracies.

So we also now are facing in an era of new data sources, so a lot of people have cell phones and wearables, and some countries are deploying video surveillance, lots of people use social media, internet searches and news, crowdsourced symptom self-reports. A lot of apps ask you to report symptoms.

So the question is, is it unethical not to use available data? Not just ethically justifiable to use the data, but also ethically obligatory? And if we were going to use the data, how do we use the data? So my colleague Michelle Mello and I, we wrote a piece for Science in their policy forum that was published I believe in April this year. This discussion is based on the Science article.

There are several innovations with new technology that are used against COVID-19. So the first one is really disease modeling and forecasting, using machine learning. So this is somewhat controversial. For example, Alibaba's Alipay, they basically capture individuals' time spent at risky locations, and the frequency of contact with another person, to generate a report, and so that if you get like a red light you cannot move anymore. They ask you to self-quarantine for 14 days.

Sometimes the algorithm really that glitches in algorithm, so people will get stuck and there's a lack of transparency in using this type of algorithms. So if you want to use the algorithm, you have to make sure that there's transparency on how it is created and who has access to it.

Leveraging and linking large datasets for case identification is another one. So as I mentioned before, Taiwan linked the immigration and customs dataset on travelers, but only for the last 14 days. So they don't use your data for last year. They only use it for the last 14 days. They send it in batch files. After 14 days, they will destroy it. So this is the limited time use for such data. So this is so that when the doctors and the nurses are seeing the patient, basically they have available of the potential travel history of that patient.

So risk-based border security, so as I enter the immigration, they also develop this individual risk assessment tool through an app. So based on your declaration they will triage you to high risk versus low risk. So whether you are asked to do self-isolation at a facility or home quarantine depends on your risk level.

The other thing that people started to use is electronic monitoring of quarantined and isolated individuals. So cell phones are now often used to do that, and there are many methodologies, and so for example, some countries use GPS data. So that's global positioning, that's a little more invasive, because they could track you anywhere. But the other countries, for example, such as Taiwan, they use cellular signals. So this is the signals that phone companies use to optimize your user experience. So you see like one bar, two bars, versus three bars, and that's your cellular signal.

So if you turn your phone off, then you have no signal and then the government knows that you turned your phone off. If you have, if your signal is outside of the location, triangulated by the cellular towers, then they know that you have left that general location.

Last time I was here, I purchased a very cheap phone and I got terrible signal. So then that day, I got visited by the police, the health department, and the local ward all on the same day, because they thought that we had left our location, but really it was the signal that was terrible.

Other countries, they have used facial recognition tools in public spaces, and I think it's of concern, because it could be used for something else, as well, for different purposes. There is enhanced contact tracing that is used, and many of you have mentioned Singapore, the TraceTogether app using Bluetooth technology, and as well as the new Apple/Google app. Now my understanding is that Singapore's adoption has not been so great. It's between 20 to 30 percent, and so for this kind of Bluetooth technology to really take off, you really need about 60 to 70 percent adoption.

In Israel, cell phone locations are obtained on an involuntary basis, and with immediate quarantine orders. So you have to be very careful, because they are actually committing somebody to a quarantine using that kind of contact tracing technology with the quarantine orders.

South Korea as well use GPS without seeking consent.

Taiwan had used -- before Diamond Princess ship went to Japan, it stopped by Taiwan for a day, and then 2,000 passengers basically left, left the ship, and what Taiwan had done was they sent cellular messages, text messages, to people who had been in the vicinity of the itinerary of the passengers to inform them to get tested if they have any symptoms.

So there are some ethical issues raised. One is privacy. So cell phone locations and text data, except for the use of law enforcement, data are not ordinarily used for tracking down and imposing consequences on people. So this is a privacy concern, particularly if people are also wanted to -- in some countries, they also wanted to see the text messages, as well.

The second issue is autonomy, asking for permission to access personal information, usually requiring informed consent, and for contact tracing through cellular records, there are strategies; for example, you could ask people to opt in or opt out or make it mandatory, and depends on what the society believes that the best way is.

So for example, in the United States, we require people -- it's mandatory to have a driver's license to drive, but for some things that you could opt out, that you could -- it shows architecture.

There are also equity concerns. New data sources can improve representation of some populations in epidemiological analysis, but disparity could exist so that you could either over-identify or under-identify individuals due to the bias in the data. So it depends on -- I think previous speakers had discussed the penetration of cellular phones might not be so great in certain areas. So in those situations, you could be potentially under-identifying people at risk.

Minimizing the risk of errors. So because the scope of deployment and the speed in which these technologies are deployed, there are going to be glitches and errors, and if machine learning and AI are used, they are going to make mistakes. So there needs to be a correction mechanism for mistakes.

Also accountability, basically once you set up a system like that, you do need transparency and to ensure that there's a governance structure to prevent potential misappropriation of the data.

Here are some general policy recommendations. There are two principles that we have proposed. One is do not evaluate in abstract, but by reference to the counterfactual. So what would be used instead of the technology that would more or less desirable? So if you're not using the technology, one way is, okay, we have done this with shelter in place for a large population of people. So that's the counterfactual.

The other counterfactual is we have to hire a lot of human contact tracers and is that sufficient to meet the demand, the challenge of this pandemic? So that's something to consider.

The other principle is the least burdensome or the least restrictive. So given the available health resources, people's health behavior without public health orders, or the transmissibility of the pathogen and the stage of the pandemic, you could sort of decide what is the least burdensome or the least restrictive for your particular community.

There are considerations for using algorithms and certainly if you use deidentified data versus identified data, the implications are different for individuals. If you're just trying to understand local epidemiology, that's very different than to stop somebody from going out. Also, using electronic monitoring to support confined persons is something that could be possible. So when you quarantine somebody, you could still text message them to make sure they are doing okay. And I think our previous speaker had mentioned that issue, the need to care, right? So if you quarantine somebody and maybe they have the virus, should the person gets worse, you should be able to send the person to a healthcare facility to get care.

Also, using electronic monitoring to enforce restrictions on movement in the United States is somewhat problematic. The Supreme Court has held that judicial warrant must be obtained and is unclear about public health orders, whether or not you could detain somebody.

Denise Love: Dr. Wang, we are running long on time, so if you can wrap up quickly, that would be great.

C. Jason Wang: This is actually my last slide. So we should try to understand the reasons for noncompliance, and lastly, I believe that in this pandemic, perhaps we should use the optout strategy, where it's in the architecture, but you could opt out. That would probably give us further along the way. Finally, I think for any policy you should have stakeholder inputs such as

this one, because there needs to be oversight to engender trust on any technology that you use.

So I'll stop right there to see if people have questions.

Denise Love: Thank you so much. This was quite a dense panel of information. I learned technology alone is not a comprehensive solution. Scientific evaluation is needed. We need intense human interaction, but a stretched-thin workforce, and the need for leadership and building trust, all very great principles, but in practicality, it's going to be interesting to see what the discussion yields.

So Rebecca, it's your call on the public comment, because we want to have a discussion on this hugely intense information that we just got.

Rebecca Hines: Why don't we take four to five more minutes to engage with the panel, pause, open it up for public comment, and if our panelists don't mind, then we'll come back and finish discussion and Q&A with you, because we don't want to lose you, but I'd like to stick to public comment at the time of the publicly posted agenda.

Denise Love: I see a raised hand by our fearless leader, Frank Pasquale. I'm going to open it up to you, Frank, to start off.

Frank Pasquale: Thanks so much, Denise, and thanks to all the members of the panel for really richly insightful presentations that I think have contributed enormously to the committee deliberations. One of the things that I'm wondering about, that I keep thinking about when I think about the use of the digital and technology in terms of data collection, analysis, and use, to advance pandemic response, is this type of use of technology essential to the approaches of countries that have really succeeded, or is it something that is just one minor part of a much larger set of requirements, and I think, Dr. Wang, one of your studies that maybe we put out with the information for the hearing, it was mentioned 124 different specific policy actions that Taiwan took.

So what I'm really wondering about here is do you think that the contact tracing was absolutely essential or the digital aspects of this, location tracking, either consensual or nonconsensual, cell phone usage, et cetera, were they essential to Taiwan's success, or were they something that just seemed to be marginally helpful in some cases but maybe not that essential?

C. Jason Wang: I would say that it's necessary, but insufficient, and the reason I say that is that -- so Taiwan has household registration. So you actually know where everybody is, and there's like a ward chief for each district. So the public health system is set up so you get a visit by a public health official if you are sick or if you need help.

Now the reason I say it's necessary, because they don't want you to go out when you're doing self-isolation or home quarantine. So they use cellular tracking. So if you get out of the general facility of the cellular towers, they know you left that area, so they will send people after you to make sure that you don't use public transportation, that you don't have -- and you could get fined up to $33,000 for breaking the quarantine. But if you stay in, they pay you. They pay you $33 a day for staying in. So you either want to get paid playing videogames, or you want to get fined $33,000.

So basically, and they bring you food during quarantine. So basically they have adopted the strategy of being nice to people that are in quarantine and support them in quarantine. But digital itself is insufficient. But it may be necessary in our country, in the United States, because we don't have household registration. So once I land in San Francisco Airport, I hop on an Uber, nobody knows where I am, except for the Uber driver. There's nobody is tracking me after I enter our country.

So how do you know that the person has been in 14-day quarantine or not? So I think the exposure notification is one way, but I think previous panels were exactly correct, that just because you have this Bluetooth doesn't mean that you are catching the people that you really need to. What if I'm wearing a mask? That protects me so that then if all people are wearing masks, then the risk is not that high, so maybe in the human part is the central one and the technology is to assist. I think Bryant is raising his hand.

Sean McDonald: One quick note is that apps have failed of necessity and proportionality analysis in at least two other analyses. So a lot of variation by jurisdiction.

C. Jason Wang: I agree. App is not the whole thing at all. It's to assist. I totally agree with that.

Public Comment

Rebecca Hines: I'll pause here, if you don't mind. I hate to pause in the middle of this thread. There's much more to be hashed out here.

Can we please have the public comment instructions, put up? Thank you, Kim.

So we are going to pause here in the middle of the proceedings to open it up for public comment. Greg, would you like to review the instructions for the members of the public who would like to have an open phone line?

Greg Richards: Of course. Hello, everyone. If you would like to submit a public comment, there are several different ways. The first is if you joined the meeting virtually via your computer, you can go down and press the Q&A box at the bottom to either submit a written question or just a request to be unmuted.

The second option is to select the raise hand button at the bottom of your screen on the computer. If your hand is raised, we will call out your name and then unmute you, and you'll be able to give your comment. If you are on the phone, you can also press star-9 to raise your hand. If you raise your hand, we will call on you for public comments.

So far we do have a few individuals who have already raised their hands. The first, Robert Gelman.

Rebecca Hines: Thank you. So, Robert Gelman, Bob, hello, you have up to three minutes, and remind us your organization and your work, please, briefly.

Robert Gelman: Hi, I am Bob Gelman. I am a privacy consultant here in Washington. I just want to talk for a minute about a report that's relevant to what you guys are doing that's going to come out I think this week, working with Pam Dixon at the World Privacy Forum, looking at the waivers that HHS issued in response to COVID pandemic. There are several flavors of these. What we have done is looked at the authority for these waivers. We have looked at the scope of the waivers. We have looked at the process for issuing the waivers, and we have looked at some of the underlying public policy, and we've raised a series of questions that need attention.

These are not matters of urgency. There will be a long list of things that will need attention once we've gotten the bulk of the pandemic behind us, and we humbly suggest that the scope of HIPAA waivers is something that belongs on that list and that perhaps the NCVHS may be the right organization to take a look at that issue.

Thank you.

Rebecca Hines: Thank you, Bob.

Greg, it looks like Jean Bikindou, can you please introduce yourself, and you have three minutes.

Jean Bikindou: Thank you for calling on me. I have two questions about the public trust and Supreme Court opposition. I believe in the United States, judicial warrants are needed, because they help to have another trust, because without a trust I don't believe the public will have enough confidence on the government to protect our health, because they can be used by many apps to collect in first part, that can be used by many actors. I do believe judicial warrant is important to protect and to give more confidence on trust and how the government or any entity will use our health information.

Rebecca Hines: Thank you.

Greg, are there any other indications of public comments?

Greg Richards: None so far. Once again, if anyone would like to submit public comment, you can do so by raising your hand or submitting a question using the Q&A box at the bottom of your screen, and if you're on the phone, you can indicate that you would like to ask a question by pressing star-9.

At this time, there is currently no public comment requested.

Rebecca Hines: Okay. So I am going to turn it back over to Denise to facilitate the discussion for a few more minutes, and if anyone else does indicate they'd like to make a comment, we'll pause and let them in until 4 o'clock. Thank you.

Panel III – Bias and Discrimination (continued)

Denise Love: Thank you. I think we are at Bryant Karras' moment of discussion. We'll continue.

Bryant Thomas Karras: I just wanted to make a comment with respect to Dr. Wang, I think I just want to underline or

emphasize the Oxford study, 60 percent threshold that you quoted assumed that public health wasn't doing any of its efforts and that we just kind of walked away from the table. So there's assessment for modeling in Washington state that with only a 15 percent adoption, we would save somewhere between 2 percent and 15 percent of the deaths that we're currently seeing. So I think we need to take every intervention and, again, emphasizing that we add this toolkit on top of the other sets of interventions that we continue to invest in.

C. Jason Wang: Thank you for that information. You are absolutely correct. I think there are a lot of interventions that are added on top, including wearing masks and various public health interventions, and so you don't need that percentage. I totally agree. Thank you for that information.

Denise Love: Sean?

Sean McDonald: For what it is worth, there have been a number of deployments that have gotten far above 15 percent in terms of total population and have not gotten anywhere close to that. You can't necessarily -- it's difficult to measure a prevented mortality, of course, but the number of total notifications moving through the system plus the interaction with the public health system overall has led most of the showrunners of those programs to sort of debunk even at 15 or 20 or 30 percent, which is I think we're all agreeing that it's possible that this matters. It is valuable to experiment with. It is clearly not getting the job done in this pandemic, and there's a lot of value in investing in the infrastructure to try to get it right for future work.

Denise Love: So no panacea. Oh, dear.

We have a couple of hands raised. I will go to Dr. Gray first, and then Vickie Mays.

Mary Gray: I just wanted to follow up on that point. I think the challenge about any of the proximity notification or digital tracing apps is that it was never built with a sense of where it would fit in a workflow. So literally until we have a plan for the workflow of where does this fall for supporting healthcare workers' efforts to be able to not just identify in an anonymous way who you have passed on a bike path, but do you need groceries brought to you because you don't have the capacity to feed yourself? Like if that's not part of the workflow, it's worthless for a significant part of our population, that we know disproportionately is being hit by the pandemic. So black and

brown communities having an app that lets them know they passed somebody when they were doing the hard work of bringing essential services to us is -- I just would really like us to stop wasting our time with those technologies and spend it on healthcare.

Denise Love: Thank you.

Vickie Mays? Are you there, Vickie?

(No response.)

Rebecca Hines: Her mic is open.

Denise Love: She may have stepped away, or maybe her hand was left up. I'll keep looking for her.

Are there any questions from any of the other committee members? I'm not seeing any here.

So I don't even know where to start, but it's clear that things are happening, and it's clear that lots more needs to happen. So what is really going to move the needle? New laws? Or is it everything? I'm sitting here thinking of all the things that have to happen between workforce, intensity, valuation, but the legal aspects. Do we need new legislation, new laws, to move that needle? Or are the laws in place and we just need to -- Sean? I'm going to punt it to you because I don't know how to answer it. I don't even know how to ask it.

Sean McDonald: Someone said earlier I am not a lawyer, and I think that maybe because I am it is now my problem. But I hear you. I think of course there are new laws that are going to be required. There's new institutional infrastructure that's going to be required, but I think it's really important to recognize that both technology and law and sort of legal agreements are designed to be reflections of productive relationships. They're not meant to necessarily -- they cannot mandate or magically create them. So I think that there are a lot of -- there's a lot of really inspiring public health work that's already going out and that's already being done. There are really incredible ways that technology is being used to support the public health response in ways that are not invasive and don't require the kinds of complexity involved.

So yes and, but I think that the first thing that we have to do is be really serious about finding a way to link development and deployment with contextual testing and dispute resolution, and

it's not just testing for the disease, but testing for the relationship of the community, and I think that draws on previous comments. But it has to be a -- we have to approach it as its own vein of experimentation, because it's a social license and a social authority that is otherwise very difficult to get back.

Denise Love: Thank you. I see Dr. Gray's hand up.

Mary Gray: I just wanted to put on the table and underscoring my initial point which is if we worked from the premise that there is no such thing as deidentified data, how would we proceed? Because we really need to be moving forward with that assumption, and there are so many regulations that right now depend on if it's deidentified, we can do X, Y, Z with the data. That is where we're fracturing and further eroding the public's trust. So I think one of the most -- what I'd love to see this committee bring forward is a need to rethink and redefine how to work with data that is generating insights from individuals and community groups through aggregation that cannot be protected through this magical thing we call deidentification.

So we really need to look at the U.S. Census. We have good examples within government that have said that's not a thing, and how would we proceed? I do think it would then push us back to the common rule, in a lot of ways, we're not doing the basics of respecting the rights of people to be aware of what it is we're doing when we're interacting with them in an ongoing way to be able to gain insight from their social interaction. That's all the social media data, a lot of that is just people living their lives. So when we're collecting those insights from their social interactions, how can we bring ourselves to the fore and say, hey, I noticed that you're having these exchanges and be able to bring that into the way we approach education and public health, rather than feeling like we're going to be able to do surveillance largescale and getting really excited about the amount of data we can amass. Look at all the laws that are allowing that collection in the name of deidentification. That should be the first place we go and say, actually, we can identify everybody we're collecting data from. How should we proceed?

Rebecca Hines: Dr. Gray, I have a written question here from Dr. Vickie Mays. I guess she was having technical issues. Here she says my question is whether there are any policy or procedures that you could suggest that would increase the engagement of racial and ethnic minorities in our data stewardship and use of

technology, either in clinical or public health, as an example, in we work in deidentified data or in how apps are licensed?

Mary Gray: There are a couple of examples of data trusts where people and Patients Like Us is an example, even examples like Harvard's Latanya Sweeney created MyDataCan, which is now how Harvard students can know exactly what kind of data is being collected about them, and they can review that data. Those are initiatives that I think show some possibilities for policies that say anything that's aggregating at -- that's taking individuals' data and aggregating it and that's where the value is, that you should be able to control the repurposing of that data.

So in terms of community trusts, I feel like there are some models out there, Sean McDonald can speak to this better than I can, but that that becomes a way to engage community groups in addressing their own health needs. One other example I'll put on the table is APS, open APS. It's an automated pancreatic systems community that basically hacked insulin pumps, and they share their insulin pump numbers to be able to improve their insulin pump functioning. So there are these glimmers of hope that to me are places where we can turn to models for giving people capacity to share insights from the way they're moving in the world.

Denise Love: I see Melissa's hand up, and then, Rebecca, after Melissa, if there's no other questions, turn it over to Frank?

Rebecca Hines: That makes sense.

Denise Love: I will finish with you, Dr. Wang, but I see Melissa and then I'll finish with Dr. Wang.

Rebecca Hines: Correct, and if any of the panelists have any final thoughts, yeah, thank you.

Denise Love: Melissa, and then Dr. Wang.

Melissa Goldstein: I very much appreciate you spending time with us today. It's been a very interesting day, and this is a great way to push us into thinking with this final panel. I've been thinking during the discussion, Dr. Wang brought up the idea of consent and he used the words opt out and opt in, and then Dr. Gray just brought up a little bit about the idea of deidentification possibly not really existing. One of our panelists earlier in the day used the term de-aggregate, I

think, or de-aggregated data, so aggregated and then un-aggregated.

I'm wondering what we think about the use of some type of consent. I always prefer opt in to opt out, I'll be very honest with you. I am doubtful that public education campaigns work, in a producing results way. I sound utilitarian, don't I?

But what I'm wondering is how to operationalize the consent. I've also been fascinated by models that use ideas of community consent. So working with particular communities. Now in New York City, that's going to be difficult, but in smaller communities it might be possible, and I'm wondering if any of you have ideas about how to operationalize it. Is it doable? Particularly in this largescale thing we're facing now, and might face again in the future? Anyone.

Mary Gray: So I could reply to that. I've been studying a group out of Duke Health that is working with community groups to put them -- to position community groups as the beginning of that contact tracing loop but also be involved in patient support. It's called the Pandemic Response Network, and we have a pilot with 12 African American churches that are effectively going to become the brokers for those community members to be able to manage that conversation around the information that you're sharing. It can be aggregated.

It's going to be effectively in a data storage tank, and I absolutely agree with some of the comments that asking somebody to think through the future risks to them of the data that's being collected about them, that's nonsensical, but it is imaginable that we can be collecting data and having a trusted data broker who I am commissioning effectively to represent my interest, would be in a better position of being able to be the throttle on the repurposing of data without my consent and be there to be able to educate me on here are the risks and benefits that could come your way for the repurposing of that data.

I think it also really calls the question on all of the repurposing that's really about a kind of futures market. It's just selling data for selling data's sake. There's no evidence that it brings any value other than to someone being able to resell data. So I think it's the bigger question of when we're collecting something, knowing that we're only collecting it for one thing, and doing the hard expensive work of collect it again if you need it for something that you can explain to someone why

you're collecting it. It brings us back to basics, but I think we're at the stage where that's so necessary.

Sean McDonald: If I could add a little bit to that. I really loved both Helen Nissenbaum and Jasmine McNealy's work talking about contextual integrity and also the importance of ecosystems, and a lot of my work so far in data trusts has sort of realized that a lot of systems don't necessarily put a premium on validly collected data or the consents necessary. So in order for that data -- in order to become a primary broker or a rights-cognizant broker of data, you have to work in a market or ecosystem that pushes additional value into good quality or publicly agreed and agreeable practice.

So where you don't have those ecosystems, which at this moment is in most places unfortunately, public health is a small example in the sense that if the data is bad and the decisions are bad, usually the treatment and the care is not -- is affected. But in many of these sort of rights ecosystems, what we're looking at is mutuality.

So it's not just can a person be represented in a decision, but can a person meaningfully enforce the abrogation of that decision. That's the other main part of this is how do you develop leverage or legal standing to in contexts where these things get brokered, and one of the exciting potential pieces of trusts is that it does introduce this new theory of law into the way that data rights can be enforced, and that's in loyalty, standards of care, and equity, all of which are designed in a lot of instances to operate in places where regulatory frameworks are not entirely fully formed.

So I think while it's by no means a panacea, as brought up earlier, looking at these mechanisms for short stopgap places to experiment and grow is a real opportunity for this committee.

Denise Love: Thank you.

Dr. Wang, I think I owe you the time.

C. Jason Wang: I think Bryant showed a chart about the data flow, how complex it is, from testing for example, right? Testing, informing people of the test results, and who should go to quarantine and so forth. I think because the complexity of the data flow and the scale in which we're doing it, I think perhaps this committee should think about that data flow in very much detail to see how we could do this in the future, quickly, because speed is of essence, because if the virus is spreading

and we're slow, they're going to be able to transmit to many, many other people. That's the first point.

The second point is that once we identify an individual that is a positive contact of somebody or tested positive, we ask them to quarantine, we have to be able to support them, either provide food, or basic needs, so that they don't have to run out to go to work, because they still have basic needs.

So our ability to do contact and tracing and quarantine relies on the ability to support the people that we're doing, we're asking to do that for themselves and for the public, because you don't want them to go out and infect the people. So I think they are tied together, and technology could help to speed things up, but it's not the panacea. I think everybody is in agreement with that.

But the data flow is very important, making sure the data is fast, getting to the right people at the right time, I think that's very important.

Denise Love: Thank you.

Mary Gray: Could I make a request? I just noticed that Rebecca Hines had said that any of the comments in the chat would not necessarily be entered as on the record? Is it possible to request that messages in the chat, at least mine, so I don't have to say it through the mic, that they are just taken as part of the record, or do you need that said?

Rebecca Hines: It would be helpful if you have something that you want captured in the transcript to say it.

Mary Gray: Got it.

Rebecca Hines: Sean, you had an observation that I thought was noteworthy.

Sean McDonald: I think Mary did a good job, but now that we're on the spot, it's just important to remember that asking people to understand the potential for harm to them based on looking at data access is liking asking people to reverse engineer a car from seeing tires and steering wheel.

Bryant Thomas Karras: I think that one of the things that we have stood up for that very reason, Sean, is an oversight and advisory committee with representatives from different communities, underserved or underrepresented or at risk, and it

has folks from non-English speaking populations as well as disability communities and representation from ACLU, et cetera, and that advisory committee we can, with them representing the respective groups at large, we can do that deep dive and try to convey the concerns and understand, because there's so -- you said it really well. There's just too much to comprehend, even amongst folks that are in the field, it can be too much to wrap our heads around.

Denise Love: And the lead time for that, Bryant, that needs to be put in place long before a pandemic.

Bryant Thomas Karras: And it is ongoing. It's not a one and done thing. It's that oversight and advisory is something that needs to keep progressing through the evolution of a response.

Denise Love: Thank you. I think I would like to turn this over to Frank at this point.

Frank Pasquale: Thank you so much, Denise. Thanks so much for excellent moderation, to you and to Melissa for your moderating these panels, and thanks so much to the panel again for really giving us a lot of insights and sharing the time today, and a special shout out to Dr. Wang for being up at 3 a.m. or 4 a.m. which is early, I realize. I thought I was sacrificing, agreed to do a talk at 11 p.m. at Taiwan later this year, but that's really goes above and beyond, so thank you.

We have what I would like to do, we're a little off schedule, but what I'd love to do now is just to take a 10-minute break, and then at 4:23, the subcommittee will reconvene to discuss our learnings today and next steps forward. So with that, I'll see you back at 4:23. Thank you.

(Break)

Frank Pasquale: I do see it is now 4:24, so we have had our 10-minute break. And I also just wanted to doublecheck with Rebecca. I have it on the calendar or on the schedule that we should just sort of move into our final session of today of the discussion to review themes, identify potential recommendations and additional information needs.

I did want to ask, though, if there was any further questions for the last panel. But I think the last panel has now departed. Is that correct, Rebecca?

Rebecca Hines: Yes. I think we have one member of the last panel still here, Mary. And she was actually asking if we wanted her to stick around. But I thought at this point, I don't know if Rachel or Maya, you want to weigh in? but my thought was that the plan was to take some time to really, as Denise did at the beginning of her opening remarks for the open dialogue, what are our main themes? What are you hearing? Is there anything coalescing? But I do think if you have any last questions for Mary, or any other of the panelists, feel free.

Frank Pasquale: Sure. So if there are any last questions, I would just set aside five minutes for that. But if not, then we can move into our final discussion and themes. Because I have some themes I just want to surface as well. So I can start that and have others just pick up.

Vickie Mays: This is Vickie. It is my understanding that we are still open, that we didn’t close the session. So that --

Rebecca Hines: That is correct

Vickie Mays: Yes. So it is open for participation. So any of the panelists, I would love to have them add their two cents.

Frank Pasquale: Great. Great. So yes. So definitely, that will be part of our discussion as well. Great.

So to dive in, in terms of -- unless there are any specific questions for -- and now I will just ask are there any specific questions for any of the panelists. So seeing none, I am just going to go through some of the themes and learnings that I got from many of the excellent presentations today. And then open it to staff, to members of the subcommittee, and to members of the full committee. And then we can have just an open discussion. And I will be watching for hands in the participants area as well.

So in terms of thinking about some of the themes today, I think what has really emerged out of these panels, one of the main things that has emerged for me is the importance of resources and thinking about resources and the overall framework for response in respect to data policy in the midst of a public health emergency.

And so we have heard repeatedly both from public health officials and from those who are experts on data collection and use in other spheres outside of public health, we have heard repeatedly about the need for an overarching and integrated

response. You know, that is well funded. That is supported at both the federal and the state and local levels.

That is not simply securitizing the public health dimensions of this crisis, but is also looking at it from a perspective of care, from a perspective of support, from a perspective of a state that is devoted to the welfare of its citizens and all residents. And that involves something beyond simple monitoring, but that involves a much larger framework of social support.

Another thing that I think is really critical here is the learning from other jurisdictions. I have certainly appreciated Dr. Wang's presentation with respect to that. And I think that there is a lot to be done further in that area in terms of what are the learnings from other jurisdictions that have succeeding?

But also, just to balance that perspective and that idea about learning from other jurisdictions, I think what we saw today was a lot of the texture and complexity and pluralism of the US system. And so in thinking about that texture, adversity, and pluralism, about the many different ways in which different public health systems responding to COVID-19, that was really a theme of many of the presentations about learning what are conditions on the ground. Learning, for example, what is different about this crisis than others.

And I was particularly chastened and saddened to hear that there is a real resistance to cooperation that has not been seen in prior crises and in thinking about how our subcommittee and others might be able to contribute to rebuilding that trust is something that I think is a very important theme.

I think that the themes and ideas of bias and discrimination as brought forward in that panel by Dr. Gray, by Dr. McDonald, by others, is extremely helpful in terms of thinking about how we can contribute to health equity and help address health disparities which I think has got to be a major concern. So it is not two pandemics at once.

And I think that finally with respect to technology and ethics, what Professor Aleen's presentation really exemplified for me was a deep attention to and awareness of potential for destructive regulatory arbitrage in the health care field where when we suddenly call upon new entities to help us in, for example, the area of testing, do we have a health data infrastructure that is capable of addressing the new forms of data collection sharing that can occur out of those situations.

That also came to me when I thought about what happens when, for example, if we say the federal government or even other jurisdictions are disabled from certain forms of surveillance by, say, the 4th amendment or by other legal restrictions, when we squeeze that part of the balloon, do the types of surveillance that, say, gets stopped via that squeezing of the balloon, just end up in another area, right?

So for example, if one really pushes hard as from a civil liberties perspective to stop certain forms of public health surveillance at, say, the state, local, or federal level, does that mean that that simply becomes then the problems of businesses or schools or universities or others which may be much less constricting than the other areas that are sort of blocked from doing those forms of surveillance.

So since there is a question of a lot of very difficult tradeoffs that emerge out of the discussions for today. But there is also a lot of very concrete things that our panelists recommended. For example, I think Professor Ellen's points about the different types of entities down to testing and need for health privacy, awareness of health privacy rules there, is something I really think connects up with past PCS work with respect to health care beyond HIPAA.

So I see many areas for fruitful further research and development of these themes and ideas in future subcommittee work. And I would love now to hear from other members of the subcommittee about their views about the learnings from today and where we might take it forward.

Would anyone like to jump in or from staff as well? Vickie, I see your hand.

Vickie Mays: I agree with what you are saying about it was a very rich day. And I was trying to think about what should our report or whatever we are going to call it, look like. I really think we should start with data stewardship in the age of COVID. We can take our data stewardship from before, use whatever is necessary, and start interlinking in that some case examples.

So you could use the Chicago testimony as a case for how they priorities having a lawyer, you know, who is local. And when that is not present, you can then talk about what you need at a state level or federal level. So I think it would be really good if what we did was had some case examples. I think within the hearing, there are two or three things that we could pick.

The other thing I would then follow it up with are gaps. And in the gaps, what I would talk about is start with Allen's presentation about the issue of testing and HIPAA and all those things. And then to bring in some of our other HIPAA stuff.

Linda did very well last time in terms of -- Linda Kloss, in terms of some of the things that she led us to in terms of identifying things that build on HIPAA or the beyond HIPAA and include those in as recommendations.

And then I think what I would kind of end with is the issue of trust. So for me, there were just three big pieces to try and fit everything in in terms of what we have heard today. And the public trust piece, I say we should end up with it because it probably is, without it, nothing else is going to work. So we really want to emphasize, after you learned all this stuff, what you need to do in terms of public trust.

Frank Pasquale: Agreed. I think that structure is very helpful in terms of thinking through how to organize what was a very diverse set of comments and expert presentations today.

Other comments? Denise.

Denise Chrysler: I can’t hear. Were you calling me or someone else?

Frank Pasquale: You. Yes.

Denise Chrysler: Thanks. So many thoughts going in my head. I am just trying to pick one little piece.

First, thank you everybody for all of the public health representatives you have included. There were four people from health departments. And to me, that was just so important to hear people who are actually in the field, having to apply laws and comply with laws and what that is to them.

And the piece I heard, I heard two pieces. One was, I know we often -- or I don’t know, I had just arrived on this subcommittee. But I have heard often the Beyond HIPAA conversation which is a concern that public health is often not subject to HIPAA. But it sounded pretty clear that it is not the wild west out there when it comes to public health. That some of them are subject to HIPAA.

But whether they are or not, they are subject to all of their own state laws, and their ethical considerations and their

policies. And what I heard is not law or no law, but different laws. And we know they vary among states, and we often talk about the patch work that our speakers did, so that it is different laws depending on the type of data, the purpose that it is going to be used for the source of the data.

And so sort of thinking about how does one help address the multiplicity of laws. And not all of them are always consistent. And thinking about national standards. And that gets really scary, though because your national standards may mean that your most restrictive laws as far as public health access to data might be the laws that end up ruling. Because in different communities, people are on different pages when it comes to government access to data.

And I will just mention the other thing I was thinking about a lot when there was talk about data trust. And to what extent would somebody apply the data trust to public health because I always think of public health for dealing with the needs of populations need the data of the populations. And what do the studies say when you have opt-in systems versus opt-out? And what populations aren't part of public health.

And then my last point is going from that to think about, well, there may be short-term issues and long-term issues. The short-term is public health needs robust data to do its job. And the long-term is how do you build trust with people being public health that includes a community consent or a listening to people in the community about data that we do collect and how we use that data, and to who we disclose that data. Thanks.

Frank Pasquale: I really appreciate that, Denise. And I particularly appreciate your surfacing that theme about the patchwork. I remember I asked one of the panels, is there any particular thing that you find -- any law or rule that you find getting in your way or troubling you? And really, it seemed like the consensus was much more -- every particular part makes sense in a way. But the whole does not.

And I think that is a really interesting and important perspective. It is one that I find is missing in some of the health privacy conversations I am part of which are much more about talking up the diversity and the pluralism of the US structure. But it does seem as though, you know, learning from the panelists today that that could be something that needs some attention.

I see next, Denise Love.

Denise Love: Yes, and like Denise Chrysler, I don't even know how to articulate all that is in my head, so I will try. I think public health is doing a really, it seems like, a pretty good job for their local and state needs during this pandemic, even though there are challenges.

But I heard a couple of things that kind of got me. The deidentification piece, I mean that is the backbone of a lot of our administrative data. And I don't think that is going to go away. So do we need a new term instead of deidentified? It is something that is more accurate to what it is. It is repackaged data for various purposes. Because our core population data sets are clearly some form of semi or deidentified data sets that fuel a lot of the initiatives and public health reporting.

I don't think we are going to get an MPI. The need for a Master Patient Index is huge. But I think that is just not going to happen in my lifetime. But maybe others can steer me right.

And the other thing that I am working with some other groups is research. Do we need to rethink research and broaden our definition of research? Because the public health data, what I understand, liquidity for more rapid turnaround research partnerships, it is really difficult when you start thinking regionally and nationally.

So when I say, states have a pretty good dataset and system for handling their local needs like in Chicago, but putting it together in a region or across the country with this patchwork and with concerns about privacy, I don't see a lot of that happening. And I think it needs to happen more rapidly and more effectively. So I didn't articulate it well. I will let Frank translate it.

Frank Pasquale: I think that is really a great set of points. I think that there is going to be a lot of very good conversation on the deidentification question and sort of the new ways of both accurately assessing and communicating the risks and opportunities with respect to different forms of data sharing based on taking different types of identifiers out.

I think that it is something with HITECH, the Health Information Technology for Economic and Clinical Health Act of 2009, I think there was an effort to sort of say, well, we can have two modes of deidentification, one being the classic HIPAA method with the 18 identifiers. And the second being subjecting it to the review by deidentification expert. And I know we have had past

discussions on this committee and elsewhere about exactly that issue.

And I think that it is an ongoing debate with folks like Daniel Barth-Jones and others, sort of weighing in, and others, it is a really interesting technical aspect here. But I hope that we can have further conversations on it because I think that it is something -- to be accurate and to rebuild that trust or to build that trust, I think, does require ways of translating often very complex concepts from computer science and other areas in medicine to a broader audience.

And it is something in work that I have seen done on committees on data acquisition and consent at hospital systems is something that you sometimes see analogized to the role of the genetic counselor, the role eventually of the data counselor who would be capable of conveying some of these ideas in a good way. And yet, simultaneously, as one, as say, privacy advocates and others want to press the health care system to do these commendable things, those who were more in the health care finance realm are consistently saying, do more with less, do less, have smaller staffs.

Post-COVID, we are seeing many hospitals that are losing hundreds of staff because essentially, you know, there has been this huge delay of elective procedures and other things that have sort of really undermined the economic model of many hospitals.

And so this is difficult to have simultaneously a pandemic and an awareness of the incredible pressures on health data and health data collection analysis and use that are coming out of that. And I think the bottom line of many of these presentations today was that requires more commitment of resources out of the health care system that is being more and more pressured financially is difficult.

And by the way, I just wanted to mention in terms of being sure that we, as a subcommittee, are able to have some next steps out of this for our agenda for our next subcommittee, if you could send to me sort of your maybe three main bullet points out of the contributions today, that would be very helpful, I think, with respect to our further deliberations.

Because I know that sometimes it seems very fresh in mind now, but then over time, it may be less fresh in mind. So just sending me that or sending the whole subcommittee those three

bullet points out of your sense of where do we go from here and learnings from today would be really helpful.

I see Vickie with your hand up and then certainly others. If you want to put your hand up, we want to keep the conversation going. Vickie? Oh, that hand may have been from the prior contribution. So I see Melissa, your hand is up.

Melissa Goldstein: Hi. Some thoughts not necessarily in any particular order. I've always been less worried about the privacy of data within the public health system than I am outside of the public health system for many reasons. Mostly because of the legal requirements that the public health is protected. But also because of the nature of the enterprise and the people that work there.

So several of the panelists brought up the idea of human factors. And I think when we think of the workers devoted to public health and things like, people take their jobs seriously and the confidentiality of the data seriously. But they also take law seriously, right? I think with the entrepreneurialism of the apps, the people forming the apps, the people selling the apps, DC has one now. They may be in use where you guys live now.

So DC has one, and so all of my friends forward it to me and say, should I sign up for this? You have to sign up for it and download I in order to use it. So it's an opt-in system.

But there are startups that are tracing data and trying to make platforms for people to use data to do research. And I think it is all of the outside of the non-covered entities, the outside the system that is more of a danger because once data is out, it is out obviously.

Professor Allen's idea of expanding the terminology of covered entity is interesting. To use the current legal structure instead of applying something else to people that are not covered entities. So because they're not covered entities, like so if we had ended up going back in person, GW was going to require all of us to get tested at least once a month.

And the students, I think, upon coming back into the district and things like that. And I am assuming most universities have something like it. I think some universities were every week. So that is faculty.

But then students, and my mind moves forward to vaccinations when there is a vaccine. Are they going to try to require vaccines as well? That gets into a different area. But it is the same data. It is the same people which with employment and with just being a student and a university or a school or a public school.

It is kind of fascinating. We get your data because you choose to go to school or you choose this job. That could be applied to most people. Like who is not connected with an organization that can't force you to give your data? And that is a little frightening.

I liked the last panel a lot in terms of the opt-in, the bias discrimination, those sorts of things. I don't know how to write what is helpful in terms of recommendations, sticking to what is already written and updating it seems to be the most in line with what exists. I don't know what is most useful. And I guess that is Maya and Rachel that have to help us with that. What is most useful? I don't know the answer.

Frank Pasquale: Thanks so much, Melissa. I think that we are definitely going to be having some great input there. I want to be sure that I get every member of the subcommittee and committee that has a hand up. So I am going to go next to Jacki Monson and then Rich Landen.

Jacki Monson: Thank you. Overwhelming, a lot of information today that I think was all great and good food for thought. When I think I know everything, I realize I don't when we all these great experts here telling us additional new things.

I think one of the areas that was interesting to me, and it continues to come up as a trend as we have sort of explored beyond HIPAA, is the idea of the prohibition against secondary use. And I think a lot of the underlying challenges that go into trust and go into the concern that Melissa just articulated where we are concerned about it going past public health.

Or going past that third party which often times is the reason why a health care organization like Sutter, we pause and don't share data because we know what the secondary use could possible by. So that area is of great interest to me.

And I think it is something that we haven't really more than touched on in the beyond HIPAA. And so that is an area that I would love for us to further explore what that looks likes.

The idea, I think, of more regulations and the idea of FTC and the other commentary that was made by many of them, I am not sure that that is going to be the most helpful. And we have that today and the challenges. We don't even know what those secondary uses are for. Because literally once the data leaves our hands, we don't know where it is going. It could be anywhere. So that is one area.

The other areas that I think are we continue to see the same comments is transparency around both the ability to enable or allow people to opt in and also the idea of just telling them what their data is being used for. I think in reality, it is hard to do those things. And it is hard to get opt in for everything. And so that is another area where COVID has obviously highlighted that. But it is an area where we talked a lot as a subcommittee over the last few years what even consent would look like and what more transparency would look like.

So those are two other areas that I think have really highlighted today the importance of potentially continue to explore them and see what else we can do. And that is all my food for thought right now. But I have like 18 pages of notes, so I am sure Frank will have more for you.

Frank Pasquale: Fantastic. That is great, Jacki. Thank you. And I see Rich now and then Jamie. So Rich?

Rich Landen: Thanks, Frank. I want to express my appreciation to all the panelists for sharing their knowledge, their experience, and their perspective. Just a ton of stuff to digest.

But I want to limit my remarks now to just three comments. One is I am impressed with the pervasiveness of HIPAA throughout the conversation today, and specifically the HIPAA privacy. HIPAA is 25 years old, but it has really made an impact and kind of set the bar.

Not that it dictates everything, but it is at least a well-stablished reference point now around which people think about privacy of health data. But that is contrast to a lot of the points made by a number of the panelists talking about the patchwork quilt of the various jurisdictions at the various levels. And that things just do not work together as we need them to in a pandemic or in a truly rational public health system.

My second point is that the NCVHS subcommittee on standards has a project underway about the convergence of clinical and administrative data. And recently, we revisited our fundamental premise where we were just talking about health care data between providers and payers and a few other tangential aspects of that. But we included affirmatively the public health data needs and the intersection of public health with particularly the clinical workflows. But to a lesser extent with the payers as well and the all-payer databases.

So the conversation I heard today just affirms the appropriateness and the correctness of that decision to include public health in our convergence project with the standards subcommittee.

Finally, I just want to remark that it was raised several times today about the possibility of expanding the HIPAA definition of covered entity to include more of the players in the health care ecosystem and public health ecosystem. The standards subcommittee has to looked into that, and it is not simple. We will be revisiting that as just part of our work in the future, I am sure. And we will take into consideration the perspectives we heard today.

But in what we looked at so far, I would just like to share with the group that it seems no matter what approach we use to expand who would become a covered entity, it has unintended consequences that were significant and negative and counterproductive. So I am not saying not to look into that. But it is not a simple solution because it is, like so many others, so multi-faceted. Thanks, Frank.

Frank Pasquale: Thank you, Rich. And it is really helpful to get that past learning into the picture because it is a very difficult topic.

Jamie and then Bill.

Jamie Ferguson: Hi. Thank you, everybody. First, I have to apologize that I have to step out of this hearing for a short while to participate in a workshop today with NIST, ANSI, and the FDA that actually talked about privacy risk management of analytical models and artificial intelligence in health care.

And I was really struck by some of the parallels between that workshop today and these panels. So some of the things that I wanted to highlight were the emergence of alternative models for deidentification based on statistical methods that are different

from what is specified in HIPAA. And I think that is certainly an area that can be explored to bridge the HIPAA/non-HIPAA gap for deidentification.

Also, there was a lot of discussion there about the disparate impact on individuals of analytical models for public health. And how individuals can be misclassified when public health agencies have incomplete data that is frequently the case today.

And then the last point I will make is about the need to improve transparency of individual understanding of how and when information about them is collected and used both for public and private purposes. And I think there were just some very strong parallels, so I wanted to highlight those things.

Frank Pasquale: Thanks so much for highlighting those, Jamie. And before this became sort of the main focus of the PCS, Privacy Confidentiality and Security subcommittee, we were talking about AI in health care. And it is something that is near and dear to my heart. I was just actually on a conference on Friday and Saturday with scholars from China, sort of comparing the regulation of algorithms in medicine in China and the US.

And so I think that is a really important issue, and it is something that I think in the longer term, PCS will be looking to it because it is sort of exactly, as you said, as many of the overlaps, lots of issues with respect to disparities, lots of many other sort of challenges that are at the intersection of medicine, computer science, and law that really need attention from a multidisciplinary group. So thank you.

Jamie Ferguson: Thank you. And right now, there are so many uses of AI in public health and population health specifically for the public health emergency that these things have really come to the floor over there.

Frank Pasquale: Yes, absolutely.

And I see next Bill and Nick.

Bill Stead: First, I want to thank the subcommittee and the panelists for a truly remarkable deep dive over the course of the day. And I guess the point I would emphasize is one you raised, Frank, the panelists raised about the fact that the sum of parts, many of which are quite good, into a whole, and the whole doesn’t work.

And so I guess the other piece of recent NCVHS history I would point the subcommittee to is the work we did on next generation vitals. Although it is not exactly the same, it gets at the same challenge of what can you do through federal leadership that will enable a federated system to work? That will never happen without federal leadership.

And so it gets at that balance that the answer here is not going to be a monolithic national system. But there has to be some national glue or it just will not work. And the question is what is the simple national glue? And I think some of the ideas we discussed in the next generation vitals. Some of the work that has been done around things like the Bridge Initiative might be useful in the recommendations that we are trying to cobble together.

I do think the idea of a few key principles or whatever that would be like get away from the thought that deidentification is protective. It may affect risk, but it is not -- but get away from it being black and white because I think we have leaned in that direction. But we have not come up with a simple way to address it.

And there may be some simple things like that that could come into sort of a list of these are truths in today's world that everybody could recognize. And they are very simple truths that are different from what the past used to be. And that will be important if we are going to come out at some point in time with trust.

Again, I don't know how many of the subcommittee have watched it. There has really been good work on the degradation of trust in this country that dates back to the 50s and 60s when the tipping lines began to shift.

And so although the tenor of the conversations today is much more, whatever the word is, loud, the shift in trust, and the progressive degradation in trust, broadly of all things really dates back. And there are some very good books about that which I am sure you, the members of the subcommittee, are aware of.

But that is a context that is a little bit like global warming. It is a context that is going on. And whatever we do needs to take that context into account without thinking we are going to turn it around in the near future. We could conceivably slow it down in some way. But those are really the only thoughts. But it is a job well done on putting the hearing together.

Frank Pasquale: Thanks so much. And I do think that is a really helpful way of reframing it. And sort of thinking, taking a big picture to an even bigger picture, sort of talking about the idea of trust declining.

I remember there is a book by Everett Rogers called *Age of Fracture* - I forget the author, but it is about exactly this historical trend of a lack of trust in institutions and sort of rebuilding that. I think that was a real theme of the third panel which, is very helpful from Dr. Gray and others in terms of saying how do we rebuild trust. And thinking about it from first principles, rather than sort of tinkering around the edges.

So next we have Nick.

Nick Coussoule: I am going to risk channeling Bill. I knew you should have let me go before Bill. I could have hit on a couple of these points.

But I think the themes, I think the trust theme is a really big one for me. And it is really broad. I think a number of panelists, and I think even Jacki, was indicating that the sheer complexity of the kind of ecosystem is mammoth. And so the way to create trust is very complicated and takes a very long time. And so I think that is a thematic element that we need to be thinking through.

At the same time, a lot of that trust is built on transparency. And so the theme of transparency, and I would actually add not just transparency, but speed matters. When we talk a good bit, I think Bill was even just talking about our prior work in regards to vital statistics. And yes, we have a federated system. But the access to the data at whatever level you need it at, whether it be a local, regional, state-based, national, access to it and access to it very quickly can also help move things along much better.

So I think that idea of building that transparency and figuring out ways structurally to improve the patient flow of information will be really important to help build that trust, to help create that framework.

The other one that is interesting for me is the distinction between kind of the private need versus the public need. The distinction between what is good for me versus what might be good generally. And I think that is a difficult topic because

it is easy to sit back oftentimes and say, this will be great for everybody.

And then you get into the, what about me? And I am like, well, that doesn't work for me. So I think some of the challenges that we will face is how do we make it equitable and fair for individuals, and at the same time, don't lose the ability to create public good out of that. And I think that is a very difficult one that ties along together with trust and with the transparency.

Frank Pasquale: That really helps. Thank you. Thanks. I think as we are going through our comments, I think the common themes are emerging. And I think that some of the ideas of the values that should inform the project as well are emerging as well.

I see hands up, but I think those are from folks that have already spoken. And so therefore, I just wanted to make sure that I had an invitation to any staff or members of the committee that might want to say something at this point.

And then I will have one more chance if anyone from the subcommittee wants to weigh in.

Vickie Mays: I just put my hand up. I guess it would help for us to talk about what do we think we want to do? So as we center these three bullets, we have some ideas.

So I know in the opening, you talked about using the old report. Are we still thinking that? Or maybe Maya can weigh in and channel Sharon and in terms of what we want. So I guess it would be helpful to start thinking about what it is we are going to do.

Frank Pasquale: I think that our next steps, Vickie, would be to outline the bullet points from members of today. And then sort of use that outline as a basis for a collective deliberation in the next subcommittee meeting.

I worry a little bit about just having seven minutes left in our timeline to commit to too much right now. But I do think that if there are concrete next steps that anyone wants to propose in terms of for the next subcommittee meeting, absolutely I will put those on the agenda as something that we can be thinking about.

Because I think you are right. Like building on the 2015 report, The Data Needs of Communities, is one way of I think

both revising, updating, and improving expanding say the points that were made there. But this might also require something distinct.

And so I think that might be our first sort of decision points, our flow chart would be to what extent would we want to put time into that past, updating and improving past publication versus something new?

Rachel Seeger: This is Rachel. With respect to the outline, we heard so much today. One of the things that we have coming out of this hearing is a summary that is being written.

So what I would like to do is be able to get the summary, kind of think about an outline along the lines of the key points that not only we heard during the hearing and hearing all of your excellent Q and A. But also the discussion that we have had now. And then try to put a path forward.

And I think Frank is absolutely correct that we need to revisit this November timeline we have been looking at and be a little more realistic about what we can accomplish. But many of you have offered an intern or an extern. And I think we would be grateful to have a team of students available to help us, once we have an outline together, maybe look at this a little topically and help do some of the work around specific buckets that we want to hit on.

Frank Pasquale: Thanks, Rachel. I really appreciate that as a clarification. Let me just be sure that there is anyone else?

Jamie, did you want to weigh in again, or is just your hand up from before? I think it is from before. Yes.

So with that, I just want to thank all of the members of the subcommittee and committee that have joined us today. I really appreciate you investing your time today in these deliberations in learning from and interrogating the folks that were testifying today. And I think that this is really a good foundation in moving forward on PCS work for the remainder of 2020 and into 2021.

Rebecca, any last thoughts?

Rebecca Hines: I just want to emphasize that the success is due in large part due to Rachel's incredible work of identifying people and getting it all organized. And I really want to

recognize her efforts here for getting this remarkable group of people together today.

Frank Pasquale: I agree. And of course, also, a huge thanks to Rachel, huge thanks you to, Rebecca, to Maya, to Marietta, for all of your help in getting this, ensuring that we had a smooth meeting today and preparing for today. We are really appreciative, so thank you.

Melissa Goldstein: It was an amazing group of people. It really was an amazing group of people. Thank you.

Maya Bernstein: Thanks, everyone. I guess we will have a meeting soon.

Frank Pasquale: Great. So we will be adjourned. So thanks very much. Have a good afternoon or a good evening. Bye.

(Whereupon, the meeting adjourned.)