From: pnt-eo@list.nist.gov on behalf of Scott David
Sent: Friday, July 10, 2020 3:23 PM
To: pnt-eo@list.nist.gov
Cc: Scott David
Subject: [pnt-eo] Profile of Responsible Use of PNT Services
Attachments: 2020 July 10 NIST Contact Tracing Adoption Test Suite.pptx; 2020 June 26 IRRI Atlas of Risk Maps with Compressed Pictures.pptx

Hi Folks - Please see attached.

Please note that some of this material makes specific reference to "contact tracing," but the issues raised in that context are also applicable to the use of PNT services generally.

The use of PNT services provides additional insight that can help to de-risk and leverage future interactions. In zero sum settings (with winners and losers) that additional insight comes at the expense of causing an intrusion on the subject of that insight. We call this the "insight/intrusion slider." In those contexts, it is necessary to manage the rules of the game to create a reasonably level playing field. Market trading, etc. are examples of win/lose interactions affected by insight/intrusion imbalances.

In "public health" and similar contexts, the rules can change to be a "non-zero-sum game" (a win/win situation), since everyone is affected negatively by disease. In that context, "use" of the system is to everyone's benefit, encouraging more expansive permissions, etc.

From this simple dichotomy emerges important guidance on strategic engagement with PNT services. Since most PNT services will depend on humans to cooperate (by loading an app, providing permissions for use under local data security laws, etc.), merely technically-feasible solutions will not provide sufficient incentive for people to participate. This is not a problem in those jurisdictions (and those emergency settings) where government compulsion can force adoption and compliance with PNT protocols. However, those situations are anticipated to be in the minority, particularly in the US.

Short Powerpoint deck presents comments that PNT services need broad deployment among relevant stakeholder groups to be effective. That broad deployment requires that the systems be both technically feasible AND BOLTS reasonable (see attachment for description of BOLTS).

We are in process of developing "BOLTS" test suite for contact tracing. Perhaps that test suite could be adapted for more general application in PNT services generally.

The second attachment is the UW APL IRRI "Atlas of Risk Maps" it is still a draft, and it lists over 500 vectors of information threat and vulnerability, collected over more than a decade, that have undermined function of technically feasible systems. In the PNT context, the Atlas provides a handy checklist of potential issues to include in a standard, or at least to explicitly declare as "out of scope" so that the standard is not considered more authoritative than intended.

Please let me know if you would like to discuss the materials further.

Kind regards,
Scott

Scott L. David

Executive Director
Information Risk Research Initiative
University of Washington - Applied Physics Laboratory