SFI TRANSMISSION

COMPLEXITY SCIENCE FOR COVID-19

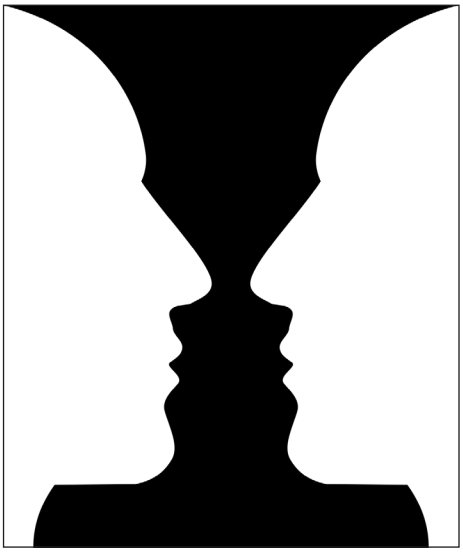
STRATEGIC INSIGHT: **Complexity science and computer algorithms can help us address privacy concerns that arise with the pandemic.**

FROM: **Stephanie Forrest, Arizona State University Biodesign Institute**

DATE: 20 April 2020 **NO: 017.1**

Pervasive surveillance is quickly becoming the new normal, whether the surveillance infrastructure is developed by governments for control (e.g., in China and many other authoritarian countries) or by large tech companies for profit, as we see in the US and other Western countries. In the age of coronavirus, these are tempting tools to turn to, either to stamp out misinformation (censorship) or for efficient contact tracing of infected individuals or detection of social distance cheaters (surveillance). One recent example is the company Kinsa, which markets an Internet-enabled thermometer and made headlines in March when it announced that it had used data from 1 million thermometers to create a national map of fever levels and had spotted a downward trend in fevers, ahead of data reported by public health agencies.

Many of us would like to contribute to databases such as these, which can play an important role in the current epidemic; however, many are wary of Internet-enabled surveillance and wish there were a way to participate without sacrificing anonymity and privacy.



Cranium Head Optical Illusion

Complex systems thinking can provide new ways of thinking about these problems. Several years ago, we studied how the immune system learns to distinguish self (its own naturally expressed proteins) from other (cells and molecules associated with invading pathogens). Put very simply, the immune system uses a trick that is reminiscent of classic figure vs. ground examples, such as the famous picture that is

both an urn and two faces. In effect, the immune system builds a map of self (the urn shape) by constructing many small detectors that represent non-self (the two faces). In immunology, this is known as "negative selection" or "clonal deletion." This simple idea can be mathematized and coded as a computer algorithm in an approach that its inventor, Fernando Esponda, calls "negative surveys."

In terms of the thermometer example, suppose each thermometer recorded the correct temperature but reported a value to the database that was different from the actual value. With sufficient data, it is a relatively straightforward calculation to recreate a histogram of the original temperature frequencies. A similar trick can be used to disguise the location from which the temperature was recorded.[1,2,3]

Such an approach would work well for problems like crowd-sourcing fever maps, but contact tracing poses a greater threat. Epidemiologists argue that the most effective way to control epidemic spread through a population is with rigorous tracing of contacts. In today's world, the most efficient way to accomplish that is by inspecting cell phone data, since almost everyone carries a phone almost everywhere they go. And some countries are indeed taking this route — for example, China, South Korea, and Singapore. In the US there are already calls for us to adopt this approach, and we are seeing an explosion of "privacy preserving" apps for contact tracing. Because cell phone data reveal much more information than that which is required to alert and test all at-risk contacts, the potential for abuse is high.[4]

Suppose that I am secretly meeting with a potential new employer, keeping an appointment with my mental health provider, or perhaps having an affair that I don't want my spouse to know about. In these circumstances, if one of my contacts becomes infected, we would like a computation that can identify every person whose location data intersects with that of the infected contact, and we don't need to know who the infected person is or what locations exposed me or my other contacts. This problem is known as set intersection, and Ni Trieu[5] and many others have developed private set intersection algorithms that use cryptographically secure methods to compute set intersections without revealing members of different sets to one another.[6] Despite the urgency of the current situation, this is the time to insist on strong guarantees (on both data collection and use), and on secure methods for computing and alerting contacts.

These are just two examples of how complexity science and computer algorithms can help us address the many privacy concerns that arise with the pandemic. In the past, we have gone to war to defend the principles of a free and open democratic society. Putting in place poorly thought-out massive surveillance schemes puts these principles at risk. Instead, we should develop and deploy methods, many of which already exist, that allow us to recover the information we need in order to preserve public health without jeopardizing our right to be free of unreasonable search and seizure.

REFERENCES

1 https://forrest.biodesign.asu.edu/data/publications/2012-percomm-neg-survey.pdf
2 https://forrest.biodesign.asu.edu/data/publications/2012-percomm-neg-survey.pdf
3 https://forrest.biodesign.asu.edu/data/publications/2011-kipda-infocom.pdf
4 https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world
5 https://nitrieu.github.io/
6 https://eprint.iacr.org/2019/634.pdf

Read more posts in the Transmission series, dedicated to sharing SFI insights on the coronavirus pandemic: santafe.edu/covid19