

NEGATIVE SOUSVEILLANCE

CARSON REYNOLDS

University of Tokyo, Department of Creative Informatics

carson@k2.t.u-tokyo.ac.jp

Abstract. Recent catastrophes have increased the desire to get rapid information about infrastructure such as power and services and not necessarily from the people providing these services. While news sources seek to provide such information, they are biased toward providing information that increases reader or viewer interest. Sousveillance is appropriate in these cases and here we describe an unusual method for such observation, which we call negative sousveillance. This is observing which systems or services disappear in a time of catastrophe and reporting on their disappearance.

1. What Disappeared?

Mann's development of "watchful vigilance from underneath" is useful in cases in which the surveilled feel that information may be used to harm them. But what of the special case in which the disenfranchised feel that information is being withheld from them?

Amid the recent earthquake, tsunami, and nuclear power crises of Japan in 2011, several individuals have expressed to me the feeling that they "are not being told everything." Indeed, Wikileaks's (Pilger, 2010) recent diplomatic cable archive documents the extent that governments and organizations routinely keep politically delicate details out of the public eye.

Negative databases (Esponda, 2006), on the other hand, are designed to solve a different problem altogether. That is the keeping records which if stolen do not reveal the identity of individuals. Negative databases achieve this by storing the complement of the set of what is being tracked. Essentially the database shows what isn't of concern.

The work of Trevor Paglen, involves long-distance photography and data analysis to document secret installations. Extending his approach the negative intelligence gatherer would seek to understand what websites, infrastructure systems, environmental sensors or documents have become unavailable.

The negative sousveillance concept then is to record, track, or infer what isn't there. This essentially suggests a two-stage process. The first step is citizens or activists to survey or map infrastructure systems or environmental status. Paulos, Honicky, and

Hooker (2009) showed how urban populations could use mobile phones as dense environmental sensors for citizen science. Analogously, Bonanni et al. (2010) have created a system for tracking and account supply chains and their environmental effects. Project such as OpenStreetMap have already sought to create public domain maps of the physical world. The second step is to record what has disappeared.

The approach is broadly applicable. Those interested in digital image manipulation can keep a delta showing how an image is gradually altered over time through the addition of watermarks or removal of figures from the scene. Those interested in network systems can track network outages due to disasters or *kill switches*, which would be used by governments to limit internet access (Cowie, 2011).

The practices of negative information gatherers in some cases would be similar to those of network security professionals. They might proceed by using tools such as *nmap* to scan various network services and store them into a database (Lyon, 2009). As services disappear they would then be listed in the far more interesting negative database. Those interested in environmental sensors may either try to gain access to the sensor data or distribute their own environmental sensor network. When nodes in such a network stop responding further investigation is warranted. It may be that the network node needs to be replaced, that it has been tampered with, or destroyed by environmental causes. But the absence of information is just as interesting as steady broadcast.

The anticipatory step of documenting infrastructure before it disappears is also useful in disaster situations when officials may be inundated with requests for information. I believe the question “is X inoperative” is an easier question to answer to than “what type of X exist and are they inoperative?” With careful foresight the negative database may be able to answer both questions without relying officials or outside organizations for details.

2. Skepticism & DIY Authority

The feeling of powerless that comes from lack of information can be alleviated by the realization that you yourself can gather information. While news sources, corporate press releases, and government agencies often have access to expert assessment I think it is fair to question whether such experts have biases. For instance, news outlets may err on the side of sensationalism to stir up concern about a recent event; corporations may time announcements to minimize the impact of bad news (Gross, 2004), or agencies may try to minimize widespread panic at the expense of accurate information.

One interesting aspect of *DIY* infrastructure, environment, or network monitoring is that those affected can collect and analyze details that affect them. When objects disappear from view instead of entering a memory hole they are instead specially noted as they are entered into a negative database. It is our hope that less will escape the notice of those willing to do the legwork involved in becoming authorities themselves.

References

- Bonanni, L., Hockenberry, M., Zwarg, D., Csikszentmihalyi, C., & Ishii, H. (2010). Small business applications of sourcemap. Proceedings of the 28th international conference on Human factors in computing systems - CHI '10 (p. 937). New York, New York, USA: ACM Press. doi: 10.1145/1753326.1753465.
- Cowie, J. (2011). Egypt Leaves the Internet. Retrieved from <http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml>.
- Esponda, F., Ackley, E., Helman, P., Jia, H., & Forrest, S. (2006). Information Security. (S. K. Katsikas, J. Lpez, M. Backes, S. Gritzalis, & B. Preneel, Eds.) Information Security, Lecture Notes in Computer Science, 4176, 72-84. Berlin, Heidelberg: Springer Berlin Heidelberg. doi: 10.1007/11836810.
- Gross, D. (2004). Friday Night Blights. Slate. Retrieved from <http://www.slate.com/id/2106864/>
- Lyon, G. F. (2009). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Retrieved March 16, 2011, from <http://portal.acm.org/citation.cfm?id=1538595>
- Mann, S., (1998), 'Reflectionism' and 'diffusionism': new tactics for deconstructing the video surveillance superhighway, *Leonardo*, 31(2): 93–102.
- OpenStreetMap Foundation. (2011). OpenStreetMap. Retrieved from <http://www.openstreetmap.org/>
- Paglen, T. (2011). Visual Projects. Retrieved on March 14th, 2011 from <http://www.paglen.com/pages/projects.htm>
- Pilger, J. (2010). Why WikiLeaks must be protected. *New Statesman*, 139(5015), 18.
- Paulos, E., Honicky, R., & Hooker, B. (2009). No Title. Handbook of Research on Urban Informatics: The Practice and Promise of the Real-Time City (pp. 414-436). doi: 10.4018/978-1-60566-152-0.ch028.