

Decontamination, Surveillance and Ready Made Martial Law in the Anthrax Age

S. Mann, U. of Toronto
mann@eecg.toronto.edu

M. Böhlen, SUNY Buffalo
mrbohlen@acsu.buffalo.edu

S. Diamond, Banff Centre
sara.diamond@banffcentre.ca

Abstract

We propose a panel discussion on surveillance versus sousveillance and critiques of both of these opposing viewpoints by artists, scientists, theoreticians and inventors in the wake of global terrorism, media frenzy and government witch-hunting. We propose elucidating both the reality of terror as well as the fabrication of its reality and all technologies that assist these processes. We will present strategies and preliminary responses to current surveillance issues and proposals, especially as they relate to surveillance in the Anthrax Age (mass decontamination, large-scale information collection, population control, quarantine, triage biometrics and mandatory medicinal control). The following submission reflects three reactions to this situation.

1 Background: Decontamination and Martial Law in the Anthrax Age¹

The threat of terrorism has made Martial Law seem acceptable to many. Thus in the event of a suspected release of a nuclear, chemical, or biological agent, the area, city, state, or the like, of the release, may be cordoned off to prevent victims, patients, suspects, or others who may be potentially contaminated from leaving the scene of the release without first undergoing decontamination.

Additionally, new kinds of decon facilities are being researched, and invented, as described in Canadian Patent 2303611 (anthrax-ready mailroom exhibit at Gallery TPW, July 2001, <http://wearcam.org/bradecon.htm>). Methods of statewide emergency evacuation by the armed forces are also well known in the prior art. For example, the Model Emergency Health Powers Act allows for entire cities to be cordoned off, in the event of a suspected possibility of a smallpox outbreak, or the like.

From fire extinguishers to riot extinguishers (big cans of pepper spray), the need for crowd control has been marketed as a new social order. And with fire hoses for crowd control the need for the fireman has changed from controlling fire to controlling people. Is he the firefighter cum people fighter? Or has his desire to control

fire merely evolved into a desire to control people? [S. Freud, *The acquisition of power over fire.*, *Int. J. Psychoanal.*, 13: 405-410.]

hose people down both to decontaminate them and to discourage them from leaving the area. ... victims would be given Tyvek suits, spare clothing, or even garbage bags to wear... dozens of people could be herded through decontamination lines simultaneously.²

And with that desire for dominance over people, comes the need for surveillance, to document the stripping and scrubbing of his subjects:

The identification of contaminated victims and their personal effects... Victims are also videotaped as they proceed through the decontamination line.²

This being done in a mechanized and very efficient way:

The disinfection/decontamination process is akin to “putting humans through a car wash” after first destroying their garments. Los Angeles World Airports have put in place a contingency plan to disinfect up to 10,000 persons who might have been exposed to biological or chemical substances.²

Decontamination centers at secret locations, with the ability to run people through a central intake facility, are also known in the art:

The city has taken steps to establish decontamination centers at various undisclosed locations, he said. “The equipment is in place. ... “We have to be able to shut down the hospital, filter people through a central intake where we can shower and wash them down,”²

Intelligence-gathering systems, means of controlling large numbers of people, etc., can also be applied to the management of a large-scale involuntary labour force. Means and apparatus for compelling civilians to perform mandatory work is well known in the art:

Other outstanding legal questions concern the ability to isolate, quarantine, or detain groups

²See summary of government and industry documents on decon: http://wearcam.org/decon_summary.htm

¹These issues were previously explored by S. Mann. (Exhibit Curated by Kathleen Pirrie Adams, <http://www.wearcam.org/dusting/tpw/> with help of James Fung, Sharon and Corey Manders, Felix Tang, Betty Lo, Chris Aimone, and Thomas Hirmer.)

or individuals; the ability to mandate treatment or mandate work; restrictions on travel and trade; the authority to seize community or private property such as hospitals, utilities, medicines, or vehicles; or the ability to compel production of certain goods³.

We now live in an era in which one spilled salt shaker can bring about Martial Law and strip hundreds of citizens of their civil rights, leaving us stripped naked, bleached, and bagged. The disinfection/decontamination process is akin to "putting humans through a car wash" after first destroying their garments. Los Angeles World Airports have put in place a contingency plan to disinfect up to 10,000 persons who might have been exposed to biological or chemical substances. Since a suspected terrorist incident constitutes a crime scene, all clothing removed from victims will be evidence. This means the clothing needs to be bagged, tagged for later victim identification (like triage tags) and set aside in a secure location until the Federal Bureau of Investigation (FBI) determines its disposition.

Here are some detailed examples of strategies each of the panelists will use in addressing the Anthrax Age theme:

2 Wearable Computing as a framework for Reflectionist Intervention (S. Mann)⁴

Reflectionism is a memesis/nemesis that holds a mirror up to society through the creation of a symmetry built from poetic justice. From the cyborg manifestations that mirror nature's own "human elements" to the conspicuously concealed wearable security cameras (<http://existech.com/domewear/>) worn by customers shopping in large department store complexes, Reflectionist art(ifacts), performances, and street theatre (<http://wearcam.org/adwear/>) will be presented in the context of post-anthrax societal values.

A series of performances have been constructed to explore issues of sousveillance⁵ in the surveillance age.

Computational clothing is perhaps the anti-thesis of mass decontamination (stripdown), and it is the computational clothing that makes the cyborg, as an element of individual performance space.

In one performance, text, graphics, and other content containing images from the hidden camera are integrated on-the-fly and rendered to the data projector for the au-

³Testimony of Margaret A. Hamburg, M.D. Subcommittee on National Security, Veterans Affairs And International Relations Committee on Government Reform July 23, 2001

⁴supported in part by the Canada Council for the Arts, with James Fung, Sharon and Corey Manders, Felix Tang, Betty Lo, Chris Aimone, Thomas Hirmer, Angela Garabet, Adwait Kulkarni, and Samir Parikh

⁵"Sousveillance" (inverse surveillance, from the French word "sous", meaning below, and "veiller", meaning to watch) is an attempt to balance the one-sided totalitarian nature of organizational surveillance.



Figure 1: The wearable apparatus contains a 1 GHz P3 CPU, rendering engine, high-power mercury vapour arc lamp data projector, within a black flame-retardant Nomex (TM) uniform custom tailored to fit the wearer. Here a person can see his own image together with other computer generated material.

dience. Provocative text messages such as "ADVERTISING IS THEFT of solitude" are mixed with video from the concealed night vision camera system (See Fig 1.).

Challenging the notion of surveillance, along with role reversal (surveillance versus sousveillance), gives rise to a reversal of performer versus audience. Passers-by became street performers and artists on the wearable stage that reflects their images to them. The stage itself, ordinarily thought of as a piece of architecture, has become a piece of clothing. Of course, the ability to play with or walk away from the situation and not participate mitigates the invasiveness of the sur/sous/coveillance.

3 Biometrics, Identity Validation, Data Flavoring and The Keeper of Keys (M. Böhlen)

Computing systems are cultural artifacts. They are conceived in and based on very strict and limited notions of what reality is and how to represent it. Devising systems that practically address the limitations and skewed assumptions built into computing systems and their practical applications, in particular where socially sensitive, biometric data is collected, managed and interpreted, is a form of cultural engagement.

With advances in imaging technologies and classification techniques, biometrics and bioinformatics promises accurate and universal identification. Uniqueness of

record is the key upon which biometric based identification and verification are built. The lure of the perfect solution by flawless identification can phase shift the consequences of potential error into insignificance or collateral social damage. But flawless technologies do not exist. Even the best and most elaborate biometric systems work with margins of error. Moreover, the convenience of electronic mass storage makes no distinction between a casually collected data entry and a permanent record. Who owns a routinely collected finger scan whose electronic permanence can exceed the time frame of its human originator? Why is the iris scan, used to ensure one's immediate credentials, silently stored beyond its use with no expiration date? And finally: Which forms of beauty can be construed of this unclaimed data?

Technologies that become prevalent create in the wake of their realization new ideas and values. This process is occupied by issues of power and politics, usually to the exclusion of any other topic. It need not be so. Image processing, for example, can be used to identify suspects captured on video. However, image processing algorithms not linked to a database or cross-referenced for suspect search have a neutral flavor. Removing external linkage from surveillance technologies by feeding all data in closed loop form back into the system changes obtrusive surveillance to observation, to a keen and attentive gaze. In a similar way, one can reclaim the territory of biometric validation and identification for non utilitarian temporary poetic purposes.

3.1 The Keeper of Keys

The Keeper of Keys (KK) is an access granting machine and data management system that utilizes finger scanning and pattern matching techniques to access a person's presumed right to enter a restricted site ⁶ Of all biometric validation techniques, finger print classification is the most established and entrenched in law enforcement through out the world. New imaging technologies replace the fingerprint with the digital finger scan, and use computational similarity measures to match one scan to another. KK makes use of this technical knowledge and differs in its interpretation of it. KK has a defined policy of data acquisition and retention, a particular conception of biometric based uniqueness and works within the laws of data classification within system inherent limitations.

KK has a vending machine style presence (Fig. 2). Appearing as a large box, a single large screen is display and interface. An industry grade commercial finger scanner⁷ is integrated into the front, between a set of speakers to the left and right. A computer, a data projector and a set of mirrors redirecting the data are housed within the apparatus.

KK is a doubled system. It operates in different modes at different times. During normal business hours KK acts as a functional and reliable gatekeeper to an area of restricted access. It employs the standard biometric valida-

⁶This work is being realized with J.T. Rinker, Ph.D. student in the Music Department, SUNY Buffalo.

⁷This project is supported in part by Ethentica Corp.

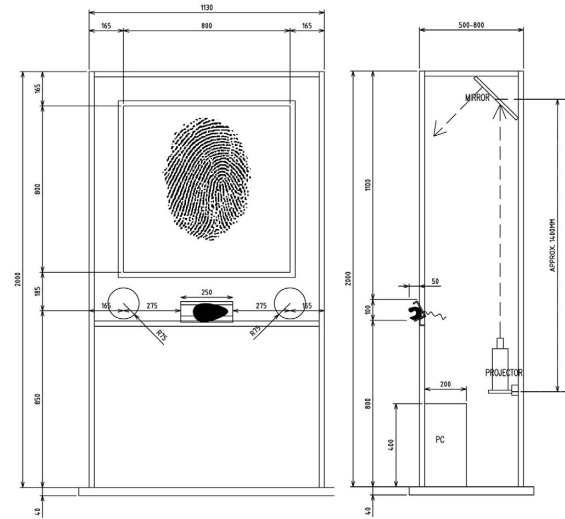


Figure 2: Schematic of KK

tion scheme of data acquisition, feature extraction, feature comparison and classification. The scanner is a capacitive imaging device that can capture a high-resolution image of a fingerprint from a hand desiring access to a given site. The minutiae points, essential features traditionally understood to uniquely characterize each and every finger, are extracted from the image. The minutiae template is then compared with those of reference finger scans previously accepted by KK.

Based on the result from the minutiae feature matching algorithm, access is granted or denied. Informed of the theoretical possibility of erroneous classification, the system varies the probabilistic strictness of its matching criteria and makes this known to the onlooker. KK can celebrate its data and hint to the user that a different data management philosophy can exist. To the utilitarian daytime construction of KK, false rejects are as undesirable as false accepts. As in all standard biometric validation procedures, reducing the possibility of false rejects increases the chance of false accepts (and vice versa). Potential instances of either category are placed in a temporary repository.

After hours, KK manages its temporary record sets per default according to different rules. It gives the collected data autonomy and group identities based on the results collected throughout the day. At night, KK massages the ambiguous potential of the day's scan work. One can think of this as a kind of artificial flavoring for data, data flavoring. Diligent and meaningful enhancements can make insipid raw data interesting. This is a return value the system gives to those who engage it. Images of poor quality scans can slide across the screen in search of like categories. Images of rejected entries are boxed into corners and asked to expire, but may refuse to do so. Over time, the rejects visually evaporate or fossilize into the domain of deleted data. There is no design for storing image material for over one day. Data misuse is prevented on the design level.

At times, the finger scans are passed to the SightSinger.

This module composes from rejected finger scans audio artifacts. The algorithm designed to perform this operation extracts salient image points from the scans and maps this information to audible frequencies in the time domain according to the KK's compositional preferences. The fingerprints thus become characteristic audio artifacts.

KK is a functional machine designed to re-imagine, beyond the confines of security and repression, notions of machinic identity control and biometric validation. It is a granter of access, a transformer, enhancer and a destruction mechanism for sensitive data for the age of large-scale information collection and population control, expanding the notion of what computing systems can be used for.

4 Intimate Technologies and the War Zone (S. Diamond)

AGENT ORANGE/ORANGE AGENCY

The Fashion of Statelessness, War and Responsibility in the Mobile Era

President Bush, please tell me, "Is Orange the Colour of EVIL?" How do we understand the colour orange, a secondary colour, and hence a result of effects, in relation to the problem of agency, of visibility and invisibility, of belonging and not belonging? How can we connect wearable technologies, the mobility of fashion as style, the desire to subtly wear communications on our sleeve or on our bodies with an era of localized warfare, globalization and the reordering of identities? The technologies of the self are core to war.

Can you shake the images of ElQueda prisoners held in the hot cages of Guantanamo by the US military? Stripped of cultural representations, dressed in vibrant neon orange, these men both live out and symbolize the loss of state protection, a spiral into the virtuality of the global political vortex. They are not the only prisoners who wear orange. In Canada, you can see the mostly Aboriginal prison population toiling at the side of the highway in work gangs, wearing flame coloured orange coveralls. They too were systematically stripped of cultural expression that includes spiritual as well as linguistic identity, ideology and ethics. They too were stripped of nation status. They have resisted. Is the era of ubiquity a return to feudalism, for some? (See Jamie King, MUTE's articles on statelessness).

What does it mean that fundamental rights that date back to the bourgeois revolution are suspended?

A friend of mine, Shawn Singer, enters the office where I am writing. He is a beautiful man; a traditional dancer and now a fashion designer whose cultural background is Blackfoot and African-Canadian. He is wearing an orange shirt with a bead collar that he has created. We talk about orange. He endorses its amplifying effect, the sense of presence, the absolute quality of the colour even if it is a mix of yellow and red. Locate expressiveness against Orange, the UK communications company that patented a colour. Orange. Global trademark of ubiquity. <http://www.orange.co.uk/register/register.html>

Orange has its history as a colour of modern war. Vietnam was a war that Americans needed to make invisible once it had ended. Agent Orange, actual chemical warfare, impeded this; these weapons of mass destruction indicated the vulnerability of American troops. Remember VietNam? Remember Agent Orange? http://www.softvision.net/ao_vets/

Before 9/11, I described an impending and now recent event at The Banff Centre, Intimate Technologies, Dangerous Zones:

Intimate Technologies/Dangerous Zones focuses on the developing invisibility and ubiquity of technology in our lives, and their aesthetic and ethical corollaries. Mobile and wireless technologies seem to be overtaking laptop and desktop, and computer creators are now designing wearable, personal technologies that adapt to a variety of personalities and uses, effectively creating new, virtual, social spaces. Young people have made great use of mobile phones, creating powerful alternate communities and languages. Cheap, mobile technology seems to be a model for sustaining the peer-to-peer revolution. The immaterial aura of signal and bandwidth influences the very fabric of our beings, moving us into a realm of constant connectivity—a dangerous, seductive zone—where the frontier between liberty and control, mobility and invasiveness, utility and disjunction, comfort and menace is blurred and leaking. We will look at wireless mediation in all areas of human life, working towards anthropology of usage. We will strive to understand how intimate technologies transform our selves and the way we tell stories, relate, play and work, and how to create positive applications and experiences for these ubiquitous networks and technologies.

Design practices and outcomes are alarmingly gendered, despite the work of researchers such as Sidney Fels, who looks at embodied and unencumbered technologies of intimacy. If men play at cyborg, as engineers, designer, military machinists, then women play at the utilities of flirtation and seduction, the intimacy of emotions in the context of wearable designs. -

One thread returns to notions of the individual, their ownership of space and notions of statehood and identity. Privacy is a construct that hangs in part on the achievements and constraints of the social transformations and resulting bourgeois revolutions of the 17th and 18th centuries. It stands hand in hand with the establishment and strengthening of the nation state. Ideas about citizenship, belonging and related rights are integral to not only identity, but the design of identity, in architecture. As Gilles Lanes has pointed out, the Reformation, with its religious dissent, required an architecture of privacy. Labour, fashion and art historians have chronicled the organization of the bourgeois family and a division of labour that included domestic labour. Clothing becomes a representation of mobility, privacy, individuation and finally, access to citizenship.

My discussion will centre on ways that intimate technologies, especially those within wearable design play against, emulate and resonate against the absolute orange of the technologies of war fashion.