Experimental Interaction Unit: Commodities of Mass Destruction

Anuradha Vikram
Curator and Critic
P.O. Box 5041
Richmond, California 94805 USA
durgaakv@gmail.com

Anuradha Vikram

ABSTRACT

This paper describes several projects by the now-defunct Experimental Interaction Unit that use product design, software engineering, and digital networking to uncover collective behaviors that contribute to systems of social control. Biology and human behavioral studies are essential aspects of this critique. Experimental Interaction Unit's projects from 1996 to 2001 represent subversive use of technology to reveal unrecognized aspects of human interaction with networks, such as how telematic distance psychologically absolves individuals from taking responsibility for their actions. The fear of vulnerability to terrorist actions, including biological warfare and electronic interference, is exploited in these works, in order to expose the ways in which security is promised in exchange for control.

Experimental Interaction Unit: Commodities of Mass Destruction

An investigation of the relationship between monitoring and accountability is central to the work of Experimental Interaction Unit (EIU). Like many contemporary artists working with new media technologies, EIU founder and primary artist Eric Paulos has a substantial understanding of the ethics as well as the scientific concerns that inform the medium [1]. Apprehensive of trusting in machine, industrial, or government architectures, he indulges the temptation to do so long enough to make a point about the seductiveness and dangers of willfully giving up self-determination to any system of control. Cloaked in a narrative of itself as a research organization rather than a single artist's project, EIU is modeled after government contractors, and like the agencies it mimics and parodies, it provides a complement of market-friendly text to accompany each project. EIU artworks, particularly *Dispersion* (1999) and *Limelight* (2001), are promoted as techno-savvy consumer products for the new age of private security.

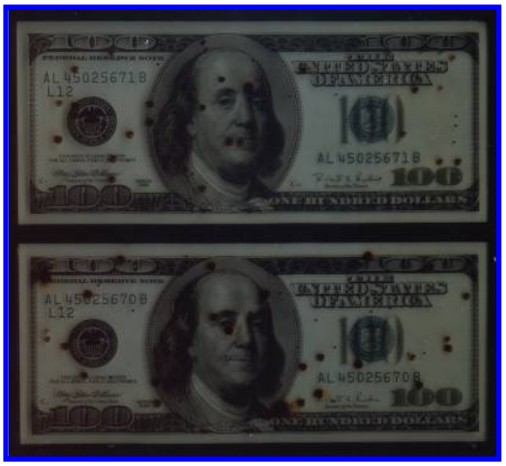

Figure 1. *Legal Tender*, © 1996 *Legal Tender* Mark Pauline, Ken Goldberg, Eric Paulos, John Canny, Judith Donath.

Paulos founded EIU in the late 1990s, during a period of collaboration with the seminal performance group Survival Research Laboratories (SRL), known for constructing tableaux of destruction in which machines go to war with one another. Whereas an SRL show presents conflict as spectacular, EIU's projects are more casually encountered. They often appear to be both easily accessible and quite dangerous. Paulos applies his technical knowledge of robotics and software to build machines that invoke the fear of terrorism and invite audience participation in threatening activities. These include dangers to physical health and safety, as well as to

electronic data. EIU's projects highlight the legitimacy of these threats, the ease with which they can be carried out, and the frequent failures of law enforcement to accurately identify and prevent them. These works underscore Americans' willingness to give up their privacy for security, and question whether this genuinely makes anyone safer. They ask us to consider whether our approach to security is effective, and how its loopholes might be exploited. Positioned within an art context, these works incriminate the art institution in their criticisms. They are ambiguous, creating a gray area where representation becomes the thing itself. It is never clear whether EIU's statements are factual or fictional, as there is no empirical evidence made available on which to base that assessment.

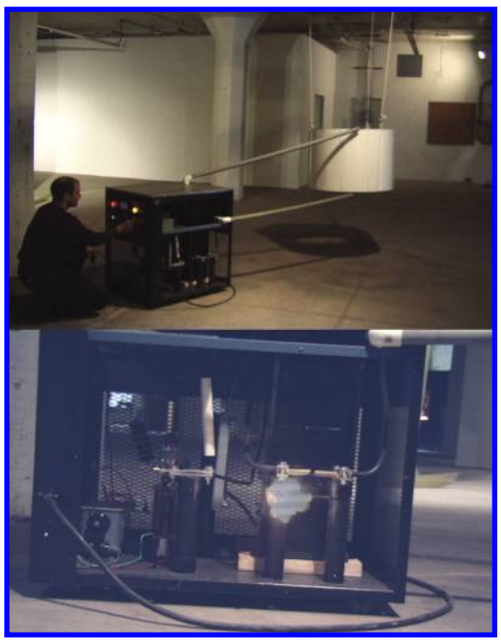

Figure 2. ***I-Bomb v2.0*****, installed outside the SFMOMA, March 2001. © 1999 Eric Paulos/Experimental Interaction Unit.**

While a PhD candidate, Paulos was part of a group of researchers based at the University of California, Berkeley, who achieved significant developments in the field of telerobotics. These engineer/artists work with robotics as a means to preserve as much of the experience of real-time action as possible over virtual distances. They construct systems involving robotic hardware, which can be manipulated and controlled via online user interfaces. The telematic systems include video, audio, and manually controlled elements that maximize the remote controller's access to visual and physical stimuli to approximate a live experience.

One telerobotic project that Paulos co-developed during this period was *Legal Tender* (1996) (Figure 1), created with collaborators Ken Goldberg, John Canny, Judith Donath, and SRL founder Mark Pauline [2]. In this project, internet distance was shown to release participants from fears about transgressing legal and social barriers, by disassociating them from the consequences of their actions. Once the participant's identity was registered in a database, the participant could, from afar, use a remote-controlled robotic arm to deface $100 bills. Paulos and Canny wrote: "This is a criminal act, as defined by United States Code, Title 18, Section 333: Mutilation of National Bank Obligations. But only if the bills are real, the web site is authentic, and the experiment actually performed" [3]. The remote participant must register his identity in order to experience the transgressive thrill of destroying someone else's money. Though it is impossible for him to verify whether or not a crime has actually taken place, he may still be culpable if it has. A primary interest in this work is to question how a criminal act can occur in virtual space, and whether accountability is preserved in the event that it does. Another is to examine our belief in the validity of an action carried out remotely, and our trust that what we see is what we know.

I-Bomb, an electromagnetic pulse-emitting device first presented in San Francisco in November 1999, was designed to demonstrate our dependence on vulnerable electronic data profiles. Data can only be damaged by I-Bomb within a radius of a few feet, so the threat is largely a symbolic one. When the electromagnetic pulse is transmitted, access to wireless networks is momentarily cut off, portable electronic devices are temporarily disabled, and magnetically stored data such as

Figure 3. *Dispersion*, installed at Ars Electronica. © 1999 Eric Paulos/Experimental Interaction Unit.

that on credit cards may be erased, creating a "technology-free zone" [4]. EIU describes this project as one of liberating individuals from economic and social pressures. The project literature makes clear that they consider this action to be a threat only to technology. "TFZ (Technology-Free Zone) systems are very selective. They do not affect organic or non-technological systems and are therefore safe for most humans" [5]. The idea of a "TFZ" recalls Hakim Bey's concept of the "Temporary Autonomous Zone" (TAZ), a conceptual space in which complete freedom from social participation, with its constraints and regulations, can be briefly realized [6]. *I-Bomb* offers one way to realize this concept, offering a space where we are momentarily freed from our electronic data *doppelgängers* whether we wish to be or not.

In March 2001, *I-Bomb v2.0* (Figure 2) appeared unannounced one evening in front of the San Francisco Museum of Modern Art, in a heavily trafficked area of the city's downtown. "Technology kills" from the event, cheekily posted on EIU's website, included erased credit cards and a wiped laptop computer [7]. The museum, though closed, was implicated as a site where technology and commerce merge to engender social control. SFMOMA is a canonical institution with great influence over the arts culture of the region. Its benefactors are enormously wealthy industrialists. Endangering their financial and social data profiles is an action that implies subversion, yet avoids real consequences. After all, the data are still preserved in the network, where they are much more difficult to eliminate.

Dispersion (Figure 3), introduced at the Ars Electronica Festival in 1999, poses an even greater potential danger to humans. "Your easy one stop choice for personal lethal biological pathogens" [8], this project appears to endorse tactics that many would consider horrific. Offering people, including children, pathogens custom-mixed to their specifications, *Dispersion* proposes to take the Second Amendment to its extreme conclusion—guaranteeing every individual access to the most advanced and lethal biological weaponry. In doing so, the project highlights the central role of civilian casualties in any act of contemporary warfare. Central to its concept is a critique of advertising and marketing strategies that manipulate the populace, by perpetuating a climate of paranoia alongside a culture of competitive ownership. Through fear and envy, we are persuaded to support corporate and government practices that are harmful to us personally. Easy access to these materials via a vending machine makes them desirable, despite the fact that no one would want such horrible stuff if he or she were thinking rationally.

The tall metal box, sized to the specifications of a commercial vending machine, is covered with glossy blow-ups of microscope photos of bacteria and viruses. One image bears the work's title and aforementioned slogan. A window reveals the robotic arm that carefully dispenses the desired agents via small plastic vials (Figure 4), and to its right is a touch-screen monitor. The user interface enables the choice of a pathogen on the basis of several factors: dispersion radius, spore survival time, infection rate, degree of contagion, desired symptoms, level and duration of suffering induced, diagnosis difficulty and vaccine availability, and mortality rate. As the user navigates through the interface (Figure 5), images of the devastating effects of these pathogens on human beings appear alongside the questionnaire. Users are led to believe that the substance they are receiving is potentially lethal and extremely potent. These substances are unlikely to be truly hazardous, but that is irrelevant. It is more important that we pay attention to the implications, rather than to the facts, of the project. The point the work makes is that people will voluntarily exchange personal biometric information for access to an object perceived as having power, because we are willing to give up privacy for the perception of defensive strength. Whether the threat that causes us to consider this trade-off is fictional or real is unimportant, because either way we begin to question long-held beliefs about our assumption of personal safety in public space.

Figure 4. *Dispersion* (capsule detail), © 1999 Eric Paulos/ Experimental Interaction Unit.

The advertising conglomerates that drive consumer societies such as ours are built on convincing people to want products that promise more than they deliver. We are in a moment as a nation when the appearance of security is frequently prioritized over verifiable results, a tendency that EIU both exploits and critiques. Security cameras and armed guards make the population feel safer, because they are perceived to be a deterrent. Soldiers with guns are still powerless against

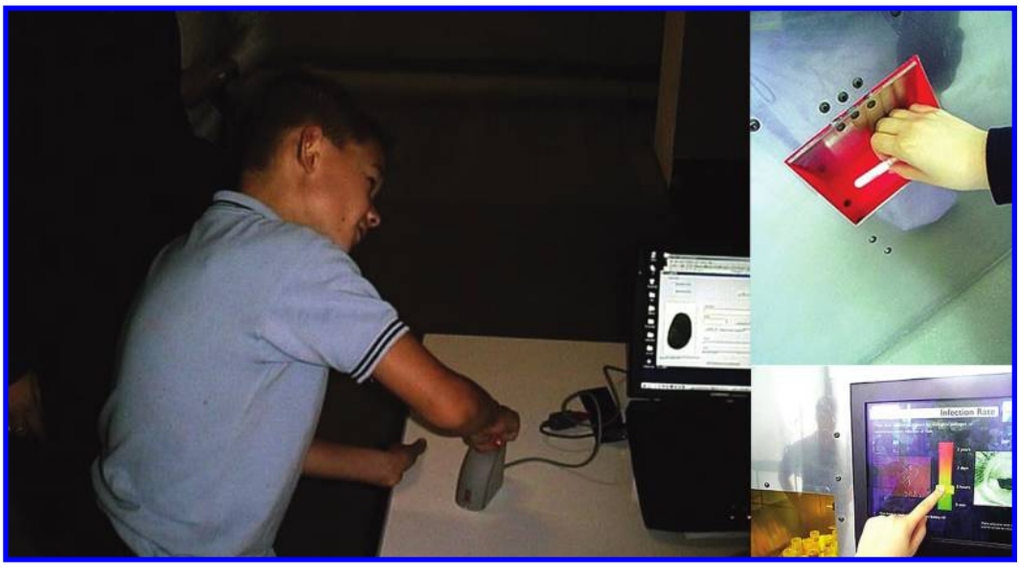

Figure 5. *Dispersion* (user interface detail), © 1999 Eric Paulos/Experimental Interaction Unit.

Figure 6. *Limelight*, © 2001 Eric Paulos/Experimental Interaction Unit.

an anthrax attack or a dirty bomb if emergency room beds are scarce and ambulance response times are slow, but these aspects of preparedness are less visible to the average person. As such, they remain inadequate and underfunded in most American cities. Another risk incurred when government and law enforcement adopt the methods of private commercial entities is that we will convince ourselves that we are protected by putting on a show of it and miss signs of impending danger that we might otherwise avoid.

All of the data provided through *Dispersion's* user interface are collected from the results of previously documented experiments and incidents involving these pathogens, most occurring at the hands of defense researchers in the USA and abroad. To operate the machine, each user must register his or her fingerprint in a database along with personal and biometric information, which is stored along with a blueprint of the agent dispersed. This information may be distributed to appropriate law enforcement agencies should they desire to monitor the recipients of any pathogens. "These systems will be required to automatically and safely cultivate, monitor, contain, package, and properly dispense lethal biological pathogens. Furthermore, the vending device must accurately record, track, and monitor the individuals using the system and observe social trends in viral demands to make long term predictions about humanity" [9]. While *Dispersion* pretends to make obtaining lethal agents easy, using them covertly would be difficult.

In this transaction, personal information is the currency, and privacy can be traded for access to the means of mass destruction. *Dispersion* functions as both a model for democratic access to terrorist methods and a data bank of potential terrorists.

EIU's final project is *Limelight* (2001), a tabletop sculpture approximately 15 inches high that promises to constantly monitor and indicate the degree of threat in an individual's environment. Taking its cue from the Department of Homeland Security's color-coded Threat Advisory System, which advises citizens to "continue to be vigilant, take notice of their surroundings, and report suspicious items or activities to local authorities immediately" [10], *Limelight* will assess the user's biometric and environmental conditions, communicate them to a central server via a low-bandwidth wireless connection, download information from databases of global threat conditions to determine a personalized and immediate level of threat, and send warnings back to the database when potential dangers are encountered. When the degree of risk is low, *Limelight* is an oddly pretty, unobtrusive object. Colored lights, sounds and vibrations indicate the threat level, becoming more intense as the danger intensifies. *Limelight*, a sleekly designed commercial product, is an appealing commodity marketed to private individuals as a protective agent. One photo on EIU's website shows it positioned next to a coffee cup, for scale (Figure 6). This is a domestic appliance.

As with previous EIU projects, protection is again bartered against privacy. *Limelight* requires a fingerprint reading to initialize and communicates any information it collects about the user's body and environment to the database. "Relinquishing this data is an important prerequisite to the overall operation of *Limelight* as it establishes a biometric guarantee of the location of the individual user. This allows for tracking, monitoring, and surveilling of the user during its operation as well as during subsequent uses" [11]. This information is recorded by the same EIU server that communicates threat warnings to *Limelight*, which profiles each user and incorporates this into its determination of the level of threat. Therefore, *Limelight's* ability to identify threats is increased when more individuals request their conditions to be monitored. Like the national ID card system proposed by many in the US and British governments, *Limelight* also positions each user as a potential threat. The safeguarding it offers is actually protection from other participants in the program.

Experimental Interaction Unit is hacking in social space. Such tactics, long employed by programmers, have met with some success in redirecting the discourse of power into distributed networks and making centralized control of power more difficult to maintain. EIU attempts to bring those distributed networks back into the physical world through their actions and to shake up centralized power in the same way. By laying bare our vulnerabilities to both internally and externally generated dangers, EIU operates in a manner similar to other contemporary art collectives including Critical Art Ensemble, RTMark, the Yes Men, and eToy. Each of these groups replicates systems of bureaucratic control and coercion, identified in the sciences and corporations as well as in legislative and defense agencies, in order to deconstruct and critique them.

References and Notes

1. One example is Natalie Jeremijenko, an engineer whose artistic practice centers on dispelling the perceived neutrality of technology. In collaborations with the Bureau of Inverse Technology, she has also worked under the rubric of a research corporation. Jeremijenko "redeploys" commercially available products for her own critical purposes. Her *Feral Robotic Sniffer Dogs* (2001-05) are modified versions of mass-marketed toy robots, which anyone can alter according to her instructions. For more information, see Timothy Druckrey, Bureau of Inverse Technology_Bit Plane, CTRL [SPACE] (Karlsruhe, Germany: ZKM Center for Art and Media, and Cambridge, Massachusetts: Massachusetts Institute of Technology, 2002) 603, and the Feral Robotic Sniffer Dogs web site: http://xdesign.ucsd.edu/feralrobots/.
2. Paulos developed *Legal Tender* while a PhD candidate in computer science and engineering at the University of California, Berkeley, under department chair Ken Goldberg. He received his degree from that department in May 2001. *ACM SIGGRAPH 96 Visual Proceedings: The Art and Interdisciplinary Programs of SIGGRAPH 96* (New York: ACM Press, 1996) 43-44.
3. John Canny and Eric Paulos, "Tele-Embodiment and Shattered Presence: Reconstructing the Body for Online Interaction," *The Robot in the Garden: Telerobotics and Telepistemology in the Age of the Internet,* ed. Ken Goldberg (Cambridge, Massachusetts: Massachusetts Institute of Technology, 2000) 283.
4. John Canny and Eric Paulos, "Tele-Embodiment and Shattered Presence: Reconstructing the Body for Online Interaction," *The Robot in the Garden: Telerobotics and Telepistemology in the Age of the Internet* (op. cit.) 283.
5. Experimental Interaction Unit, *I-Bomb:* http://eiu.org/experiments/i-bomb/tech_killed.html.
6. Hakim Bey, *The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism* (New York: Autonomedia, 1991): http://www.hermetic.com/bey/taz3.html.
7. Experimental Interaction Unit, *I-Bomb:* http://eiu.org/experiments/i-bomb/tech_killed.html.
8. *Ibid.*
9. Experimental Interaction Unit, *Dispersion:* http://eiu.org/experiments/dispersion/.
10. US Department of Homeland Security, Threats & Protection: http://www.dhs.gov/dhspublic/display?theme=29.
11. Experimental Interaction Unit, *Limelight:* http://eiu.org/experiments/limelight/info.htm.

Annotated Bibliography

Bey, Hakim, *The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism* (New York: Autonomedia, 1991): http://www.hermetic.com/bey/taz3.html.

Christopher, Roy, "ExperiMental InterAction," *Frontwheeldrive* (January 26, 2000): http://frontwheeldrive.com/eric_paulos.html. (Interview with Eric Paulos. Describes SRL collaboration and future plans. Talks about establishing trust between humans and machines through a user interface as a central element of EIU's practice.)

Critical Art Ensemble, *Flesh Machine: Cyborgs, Designer Babies, and New Eugenic Consciousness* (New York: Autonomedia, 1998). (Describes the phenomenon of technology integrated with the body and the potential sacrifices that this requires in exchange for increased human capacity. Written by contemporaries of the artists under consideration.)

CTRL [SPACE], *Rhetorics of Surveillance from Bentham to Big Brother* (Karlsruhe, Germany: ZKM Center for Art and Media, and Cambridge, Massachusetts: Massachusetts Institute of Technology, 2002).

Experimental Interaction Unit: http://www.eiu.org/. (Provides detailed descriptions and images of projects, as well as Eric Paulos' statement about the effect of the 9-11 attacks on his practice and approach.)

Federal Trade Commission, "Identity Theft Survey Report," *Synovate* (September 2003): http://www.ftc.gov/os/2003/09/synovatereport.pdf/.

Goldberg, Ken, ed., *The Robot in the Garden: Telerobotics and Telepistemology in the Age of the Internet* (Cambridge, Massachusetts: Massachusetts Institute of Technology, 2000).

Hunt, David, "Rx for Disaster," *Rhizome* (September 6, 1999): http://www.rhizome.org/ars99/9.html.

Lee, Pamela M., *Chronophobia: On Time in the Art of the 1960s* (Cambridge, Massachusetts: MIT Press, 2004).

Leopoldseder, Hannes, and Christine Schöpf, *CyberArts 99: International Compendium Prix Ars Electronica* (Vienna and New York: Springer, 1999). (Contains a section on Dispersion by Eric Paulos, awarded an Honorable Mention in the category of Interactive Art, documenting the project's presence at the festival.)

Stanley, Jay, "An ACLU Report. The Surveillance-Industrial Complex: How the American Government is Conscripting Businesses and Individuals in the Construction of a Surveillance Society," *American Civil Liberties Union* (September 2004): http://www.aclu.org/Privacy/Privacy.cfm?ID=162298c=130.
Zeller, Tom Jr., "Breach Points Up Flaws in Privacy Laws," *The New York Times* (February 24, 2005).

Zero News Datapool, "The Mythology of Terrorism on the Net": http://www.to.or.at/cae/mnterror.htm.