ISSN: 2451-8611
ISBN: 978-1-910172-00-1

Participatory (Counter-) Surveillance and the Internet

Annina Rüst

Department of Transmedia
Syracuse University
Syracuse, NY, United States of America
arust@syr.edu

Abstract

This is a text about Internet art projects dealing with Internet surveillance. In the paragraphs below, I will describe a web service that floods the Internet with fake websites, another web project that allows users to create email accounts in the names of villains that send conspiratorial emails to each other, and a solar-powered disco ball on which YouTube dance videos are projected. What connects these seemingly disparate projects? It may sound absurd, but these projects may help us understand our complicated existence as surveillant and surveillee within networked communications. Since the projects described in the text were made over more than a decade, the article may also reveal some aspects of how the Internet has changed over time.

Keywords

Internet, Internet art, surveillance, participatory, countersurveillance, detournement, humor, hacking.

Introduction

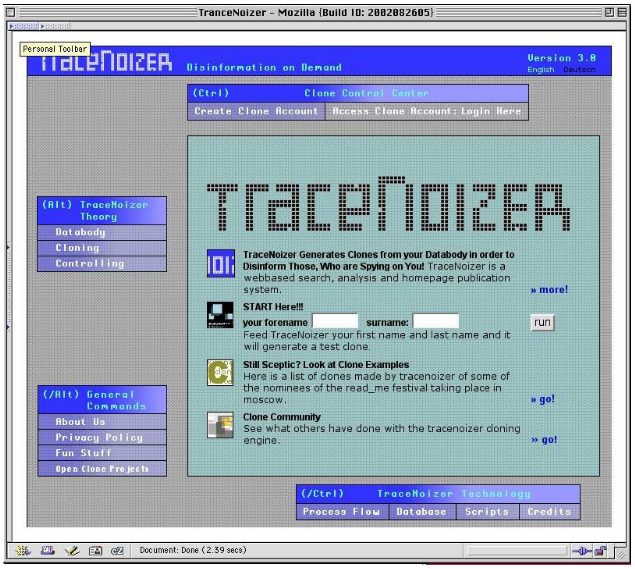
Internet surveillance is complicated. Digital pessimists tell us that surveillance is always negative, because it violates our right to privacy, free speech, etc. And yes, it does (no need for the pitchforks to be raised)! However, there are a lot of gray zones and relationships to consider. Anders Albrechtslund explains in his article "Social Networking as Participatory Surveillance" that people actively construct an identity as they share information with others in Social Networks. They are therefore not powerless subjects of a hierarchical surveillance apparatus but actively participating in mutual surveillance by exchanging information about themselves with others. This subjectivity-building activity therefore is empowering and not disempowering. [1] Albrechtslund's text gives us a glimpse into how complex Internet surveillance is. However, beyond participatory surveillance in Social Networks, there are many more surveillance relationships that we need to consider: People spy on one another using search tools, private companies spy on consumers, government agencies spy on people, and those same government agencies spy on one another. In the following, I describe electronic art projects that question Internet surveillance and shed light on the nature of surveillance relationships. These projects were made by me alone or with collaborators over roughly 10 years. I see these projects as participatory countersurveillance. As I describe the projects in the paragraphs below, I will be building a loose definition of the term.

Participatory Countersurveillance

To begin, I look back to 2001-2002. Compared to today, the Internet at the time seemed like a public park. [3] Nostalgia aside, even at the time, crucial wayfinding went through companies like Google: Then, as today, the most popular search algorithm belonged to the aforementioned company. The term algorithm is used in the context of computer programming to describe step-by-step procedures in automated reasoning and data processing. [4] The Google search algorithm determines how web content is prioritized and in what context it is shown. At the time, the basic algorithm was fairly simple: Pages with lots of links from other pages pointing to them were shown first. [5] The search engine was in the process of becoming the research tool of choice for the majority of Internet users. Thus, the verb "to google" was coined.

Search engines enable a special kind of research: spying on others. But what if you do not want to be found? As part of the group LAN based in Zürich, I created the project *Tracenoizer – Disinformation on Demand* in 2001 [6] (figure 1) to provide a tool for people who did not want personal data to be found by users of search engines. I am writing about this project in the past tense because at the time of writing the project is available as an archived version on my website, but is no longer functional. This is a fate that is typical for Internet art projects that use extensive server-side scripting.

When we created the project, we realized that all the data traces associated with a person constitute a databody. This databody consists of all the data traces associated with with a person, irrespective of whether the person has produced the data themselves or if it was produced by somebody else. We created a service to "clone" one's databody and therefore cloud one's identity. Users could enter their name and *TraceNoizer* would do a search using Google, Yahoo, Altavista, or whatever search engine was not blocking us at the time.



TraceNoizer Generates Clones from your Databody in order to Disinform Those, Who are Spying on You! TraceNoizer is a webbased search, analysis and homepage publication system.

START Here!!!

your forename ______ **surname:** ______

Feed TraceNoizer your first name and last name and it will generate a test clone.

Still Sceptic? Look at Clone Examples

Here is a list of clones made by tracenoizer of some of the nominees of the read_me festival taking place in moscow.

Clone Community

See what others have done with the tracenoizer cloning engine.

Figure 1. The *TraceNoizer* website © LAN

TraceNoizer would download the search results and run a statistical text classification using the Rainbow text classification library [7] on the data to organize the downloaded text into statistically related groups.

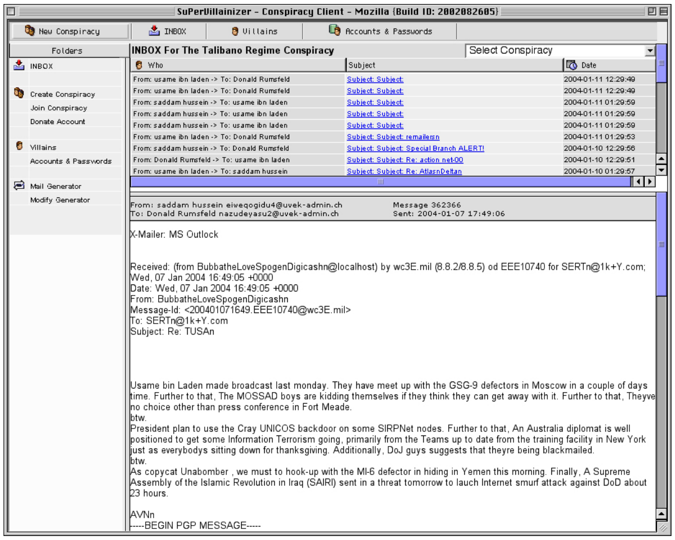
Using these organized groups of text, the program created a home page with thematically organized subpages. The website was then uploaded to a public webserver. Following this, *TraceNoizer* would run another search based on the previous search and make another slightly different website. Websites were linked to each other so that in the eyes of the Google indexing algorithm, their "importance" was increased. As a result, the sites created by *Tracenoizer* would show up in the search result when people searched for a person's name. The idea behind *TraceNoizer* was to create a cloud of disinformation so that nobody doing personal research could tell real from fake information and the original databody of a person would disappear.

Maintaining one's own databody and spying on others via search engines can be described as a sort of participatory surveillance in that the surveillee is participating in their own surveillance while surveilling others. TraceNoizer is a participatory countersurveillance tool in that it uses the mechanisms of participatory surveillance (search engines) to counter participatory surveillance.

Participatory Countersurveillance

More than a decade ago, in October 2001, the Swiss parliament issued a decree that mandates Internet service providers to retain metadata for six months [8]. This means that law enforcement agencies can reconstruct a person's social network because they have access to email and phone data. Proponents of this type of legislation tend to cite terrorism as a justification [9]. So far, no terrorists have been caught as a result of the Swiss legislation: A study by researchers at the Max Planck Institute found no statistical indication that data retention increases the efficiency of law enforcement. [10] Besides being ineffective, data retention also does not conform to the presumption of innocence, a fundamental right in a democracy.

When mandatory data retention in Switzerland was instituted in 2002, I responded by making the project *SuPerVillainzer – Conspiracy Client* [11] (figure 2). It is a webproject and the website itself still exists but like *TraceNoizer*, I no longer maintain it – one of the problems of preserving digital art. *SuPerVillainzer – Conspiracy Client* is a website that looks like a program for sending and receiving email. However, instead of facilitating the typical functions of an email client, it allows users to create email conspiracies. Users can enter a conspiracy name and a select a set of villain profiles (figure 3). Then they can press a button labeled "create conspiracy" and email addresses will be created for the selected conspiracy on a Swiss server. These email addresses will then automatically start sending each other conspiratorial emails. These emails have subject headers such as "NSA ALERT!" The body of the email will have ostentatiously conspiratorial text such as: "The informer we have inside the Secret Service says they are planning to sell details of the updated AFIWC COMPUSEC plans to the Dallas diplomat in Bern just as everybody is sitting down for Christmas dinner." Other emails look like they are encrypted. In the years when I actively maintained the service, thousands of villains were created. They had the names of the people who created them, but villains were also named after politicians, military officials, scapegoats, etc. Users created Conspiracies with names such as "Operation Blue Phoenix", "Tomorrow at 6:00:00", "The Mustafa Connection", and many thousands more.



INBOX For The Talibano Regime Conspiracy

Who	Subject	Date
From: usame ibn laden -> To: Donald Rumsfeld	Subject: Subject:	2004-01-11 12:29:49
From: usame ibn laden -> To: Donald Rumsfeld	Subject: Subject:	2004-01-11 12:29:49
From: saddam hussein -> To: usame ibn laden	Subject: Subject:	2004-01-11 01:29:59
From: saddam hussein -> To: usame ibn laden	Subject: Subject:	2004-01-11 01:29:59
From: saddam hussein -> To: usame ibn laden	Subject: Subject:	2004-01-11 01:29:59
From: usame ibn laden -> To: Donald Rumsfeld	Subject: Subject: remailersn	2004-01-11 01:29:53
From: saddam hussein -> To: Donald Rumsfeld	Subject: Subject: Special Branch ALERT!	2004-01-10 12:29:56
From: Donald Rumsfeld -> To: usame ibn laden	Subject: Subject: Re: action net-00	2004-01-10 12:29:51
From: usame ibn laden -> To: saddam hussein	Subject: Subject: Re: AtlasnDeltan	2004-01-10 01:29:57

```
From: saddam hussein eiweqogidu4@uvek-admin.ch          Message 362366
To: Donald Rumsfeld nazudeyasu2@uvek-admin.ch           Sent: 2004-01-07 17:49:06

X-Mailer: MS Outlock


Received: (from BubbatheLoveSpogenDigicashn@localhost) by wc3E.mil (8.8.2/8.8.5) od EEE10740 for SERTn@1k+Y.com;
Wed, 07 Jan 2004 16:49:05 +0000
Date: Wed, 07 Jan 2004 16:49:05 +0000
From: BubbatheLoveSpogenDigicashn
Message-Id: <200401071649.EEE10740@wc3E.mil>
To: SERTn@1k+Y.com
Subject: Re: TUSAn




Usame bin Laden made broadcast last monday. They have meet up with the GSG-9 defectors in Moscow in a couple of days
time. Further to that, The MOSSAD boys are kidding themselves if they think they can get away with it. Further to that, Theyve
no choice other than press conference in Fort Meade.
btw.
President plan to use the Cray UNICOS backdoor on some SIRPNet nodes. Further to that, An Australia diplomat is well
positioned to get some Information Terrorism going, primarily from the Teams up to date from the training facility in New York
just as everybodys sitting down for thanksgiving. Additionally, DoJ guys suggests that theyre being blackmailed.
btw.
As copycat Unabomber , we must to hook-up with the MI-6 defector in hiding in Yemen this morning. Finally, A Supreme
Assembly of the Islamic Revolution in Iraq (SAIRI) sent in a threat tomorrow to lauch Internet smurf attack against DoD about
23 hours.

AVNn
-----BEGIN PGP MESSAGE-----
```

Figure 1. The *SuPerVillainzer* website © Annina Rüst

The project was motivated by my interest in terrorist communication. I wondered, how can one tell what a conspiracy looks like? What constitutes terrorist communication? And finally: Who decides who is terrorist and who is not? How is an "enemy" profiled within a load of metadata?

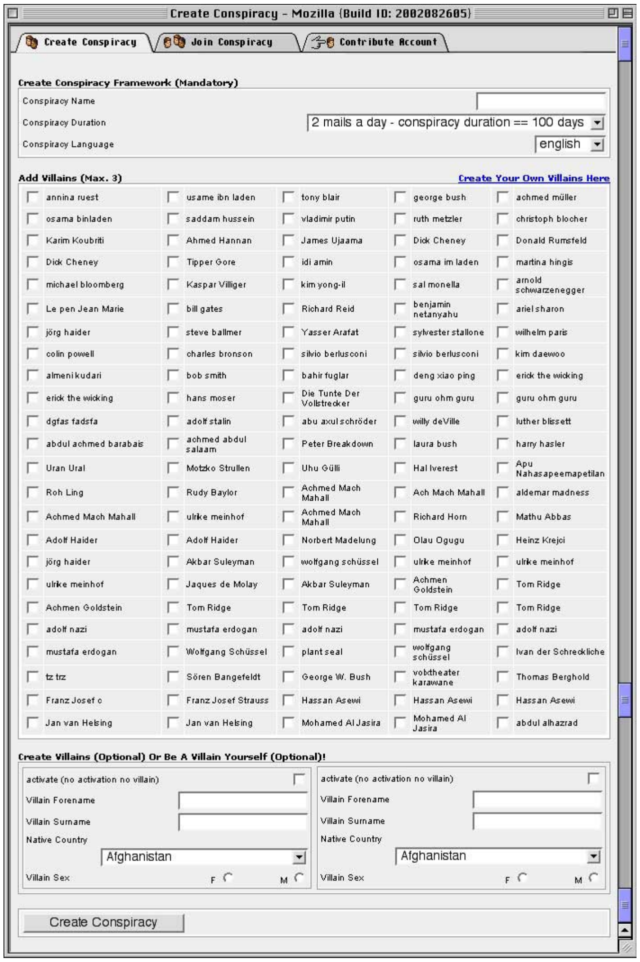
Sunrise, the Swiss Internet service provider on whose servers I automatically created email accounts eventually found out about my activities. I think that the project appeared on the radar of their legal department only when print newspapers started writing about it. They sent me a letter ordering me to stop my activities and turn over passwords and usernames for the email accounts I had generated. Of course I complied and I did not hear from Sunrise's legal department ever again. The project however continued: I set up my own server where I continued to generate email accounts.

In 2005, I created a sequel to *SuPerVillainizer*, called *Sinister Social Network* [12], a project similar to *SuPerVillainizer* in that it constituted a participatory, speculative approach to Internet surveillance. However, this project specifically focused on surveillance algorithms, specifically on programs that identify suspicious activity.

These algorithms exist. One such algorithm was outlined in a paper presented in 2004 at the 2nd NSF/NIJ Symposium on Intelligence and Security Informatics. The paper explains the rules that allow researchers to search through data from chat rooms and distinguish malicious communications patterns over benign ones. For example: "Normal communications in the network are voluntary and 'random' however a hidden group communicates because it has to communicate (for planning or coordination)." [13] (Baumes, Goldberg, Magdon, Ismail, Wallace 1). No examples of actual observed terrorist communications are given but the rules outlined by the researchers show what stereotypical "criminal" behavior would look like. The researchers are therefore building a hypothetical profile based on speculation. In his book, *The Simulation of Surveillance: Hypercontrol in Telematic Societies* William Bogard calls this kind profiling "surveillance in advance of surveillance". [14]

Like *SuPerVillainizer*, the project *Sinister Social Network* existed mainly on the Internet. I populated IRC chat channels with villains and charted their activities in a social network graph. I displayed the IRC conversations on a website and asked viewers to speculate what kinds of sinister things were going on in the chat channel.

Like *TraceNoizer*, the projects *SuPerVillainizer* and *Sinister Social Network* are participatory counter-surveillance environments. However, the approach here is speculative: Users of both websites can create speculations about who the enemy could be and whom they are conspiring with. The projects explicitly question power: I am using the projects to raise the question of who is allowed to collect and analyze communications data and according to what criteria.



Create Conspiracy - Mozilla {Build ID: 2002082605}

Create Conspiracy Framework (Mandatory)

Conspiracy Name

Conspiracy Duration: 2 mails a day - conspiracy duration == 100 days

Conspiracy Language: english

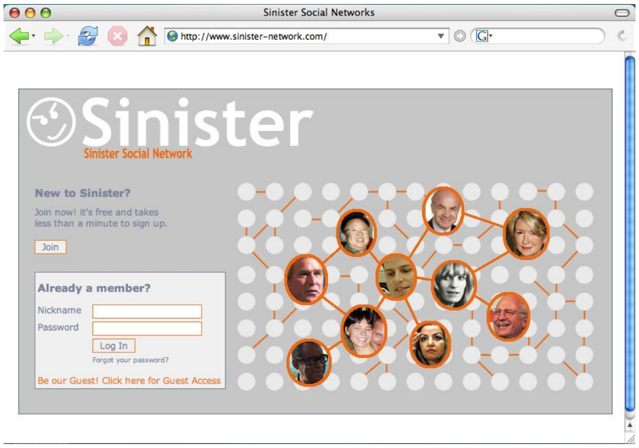
Add Villains (Max. 3) Create Your Own Villains Here

□ annina ruest	□ usame ibn laden	□ tony blair	□ george bush	□ achmed müller
□ osama binladen	□ saddam hussein	□ vladimir putin	□ ruth metzler	□ christoph blocher
□ Karim Koubriti	□ Ahmed Hannan	□ James Ujaama	□ Dick Cheney	□ Donald Rumsfeld
□ Dick Cheney	□ Tipper Gore	□ idi amin	□ osama im laden	□ martina hingis
□ michael bloomberg	□ Kaspar Villiger	□ kim yong-il	□ sal monella	□ arnold schwarzenegger
□ Le pen Jean Marie	□ bill gates	□ Richard Reid	□ benjamin netanyahu	□ ariel sharon
□ jörg haider	□ steve ballmer	□ Yasser Arafat	□ sylvester stallone	□ wilhelm paris
□ colin powell	□ charles bronson	□ silvio berlusconi	□ silvio berlusconi	□ kim daewoo
□ almeni kudari	□ bob smith	□ bahir fuglar	□ deng xiao ping	□ erick the wicking
□ erick the wicking	□ hans moser	□ Die Tunte Der Vollstrecker	□ guru ohm guru	□ guru ohm guru
□ dgfas fadsfa	□ adolf stalin	□ abu axul schröder	□ willy deVille	□ luther blissett
□ abdul achmed barabais	□ achmed abdul salaam	□ Peter Breakdown	□ laura bush	□ harry hasler
□ Uran Ural	□ Motzko Strullen	□ Uhu Gülli	□ Hal Iverest	□ Apu Nahasapeemapetilan
□ Roh Ling	□ Rudy Baylor	□ Achmed Mach Mahall	□ Ach Mach Mahall	□ aldemar madness
□ Achmed Mach Mahall	□ ulrike meinhof	□ Achmed Mach Mahall	□ Richard Horn	□ Mathu Abbas
□ Adolf Haider	□ Adolf Haider	□ Norbert Madelung	□ Olau Ogugu	□ Heinz Krejci
□ jörg haider	□ Akbar Suleyman	□ wolfgang schüssel	□ ulrike meinhof	□ ulrike meinhof
□ ulrike meinhof	□ Jaques de Molay	□ Akbar Suleyman	□ Achmen Goldstein	□ Tom Ridge
□ Achmen Goldstein	□ Tom Ridge	□ Tom Ridge	□ Tom Ridge	□ Tom Ridge
□ adolf nazi	□ mustafa erdogan	□ adolf nazi	□ mustafa erdogan	□ adolf nazi
□ mustafa erdogan	□ Wolfgang Schüssel	□ plant seal	□ wolfgang schüssel	□ Ivan der Schreckliche
□ tz trz	□ Sören Bangefeldt	□ George W. Bush	□ voktheater karawane	□ Thomas Berghold
□ Franz Josef c	□ Franz Josef Strauss	□ Hassan Asewi	□ Hassan Asewi	□ Hassan Asewi
□ Jan van Helsing	□ Jan van Helsing	□ Mohamed Al Jasira	□ Mohamed Al Jasira	□ abdul alhazrad

Create Villains (Optional) Or Be A Villain Yourself (Optional)!

activate (no activation no villain) □	activate (no activation no villain) □
Villain Forename	Villain Forename
Villain Surname	Villain Surname
Native Country: Afghanistan	Native Country: Afghanistan
Villain Sex F ○ M ○	Villain Sex F ○ M ○

Figure 3. The *SuperVillainizer* conspiracy creation tool © Annina Rüst



Sinister Social Networks

http://www.sinister-network.com/

New to Sinister?

Join now! it's free and takes less than a minute to sign up.

Already a member?

Nickname

Password

Forgot your password?

Be our Guest! Click here for Guest Access

Figure 4. The *Sinister Social Network* website © Annina Rüst

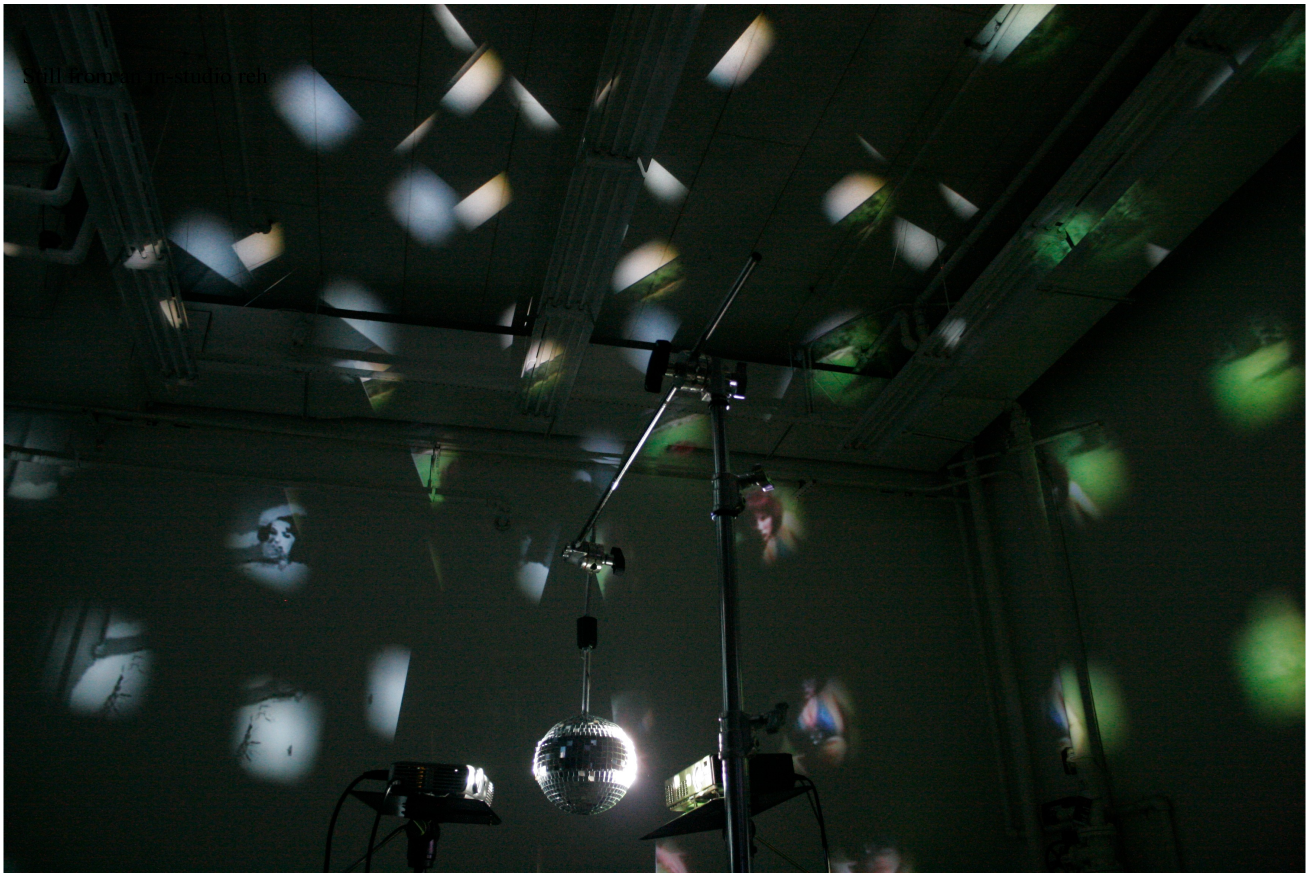


Figure 5. Still from an in-studio rehearsal of *Discotrope: The Secret Nightlife of solar cells* © Amy Alexander and Annina Rüst

Participatory Surveillance and Empowerment

In his article about Participatory Surveillance in social networks, Anders Albrechtslund says that social surveillance practices are at the heart of social networking. Albrechtslund writes that as users share information about themselves with others they build identity and subjectivity online. He sees this surveillance practice as empowering. [15]

One such example of online identity building is a genre of web video where people film themselves while dancing. On the popular social networking site YouTube, the type of video where people film them themselves has become a widespread phenomenon. Countless people are recording themselves dancing and sharing these clips through YouTube and other social media platforms. This form of online identity building differs from the online identity building that LAN addressed in the early 2000s with *TraceNoizer – Disinformation on Demand*. Today, online identity is not mainly expressed in the form of a home page on a server. Rather, it is distributed over social networking sites owned by companies such as Facebook, Google, Yahoo, and Twitter. Communication on the web today is much more widespread, visual, and exhibitionist than it was in 2001. It is still consumed in the form of text but mostly through images and videos. The following section of the paper is therefore not a departure from the topic. On the contrary, it takes into account surveillance relating to online identity building enabled by social media platforms like YouTube.

In 2012, Amy Alexander and I created the performance project *Discotrope: The secret nightlife of solar cells* [16] (figure 5), which examines the genre of the YouTube dance video. The performance features a solar powered disco ball. We project dance videos against it. In the performance we trace the genre of the YouTube dance video back throughout film history.We found that the sense of intimacy and immediacy between performer and audience that characterizes the YouTube performances was popular in early silent films and Hollywood musicals, where models for performance were drawn more from vaudeville than from theatrical narrative. An example for this is the silent film "Annabelle – Serpentine Dance" [17] shot as one of the first films in 1894 at Thomas Edison's film studio. In this clip, the dancer performs directly "at" the camera. Like in YouTube dance videos, the performer looks directly into the camera. Theresa Rizzo describes this type of cinematic performance as an "exhibitionist cinema where the spectator is overtly acknowledged and invited to look" [18]. There is an element of voyeurism and exhibitionism that can be found both in early cinema and later on in YouTube clips. We have found that this direct-to-audience style continued on to the musical films of the 1940s for example in the films featuring Ginger Rogers and Fred Astaire. Later on, films were shot in such a way where the audience takes a "fly-on-the-wall" perspective. An example for this style is the film "Dirty Dancing" where no direct-to-audience dancing takes place and the actors stay in character throughout the film. Exhibitionistic cinema has only recently come back in the genre of the YouTube dance video. This type of video is typically shot with a webcam on a computer and oftentimes in an intimate setting such as a living room, a garage, backyard, or in a bedroom. Like in the Annabelle clip from 1984, the YouTube dancer acknowledges the camera.

During the Discotrope show we project this historical trajectory onto a disco ball where mirrors have been replaced with solar cells. This creates a mosaic-like projection against the walls. When enough light hits the ball, the ball rotates and the projection rotates along with it. We perform the ball live, adding color and light to the video projections, improvising layering and mixing to create visually rhythmic stream-of-consciousness juxtapositions. The changes in imagery vary the light to the solar cells, which changes the speed of the ball's rotation, allowing us to "choreograph" the movement of the projected visuals. Accompanying the performance is an algorithmic sound design by composer Cristyn Magnus. Sound is generated and mixed in real time from the audio tracks of the projected videos, creating a seamless, danceable connection between audio and visual.

In the performance we examine how today's YouTube dancers represent themselves. We reveal contrasts and connections over cinema history. Those include characteristics such as gender and body expectations, implications of aforementioned voyeurism and exhibition. We have found that although YouTube performers are self-directed, liberated and empowered, many still will enact gender stereotypes and conform to body expectations. Dancers that successfully defy gender stereotypes such as an obese man in a leotard dancing to Beyonce's hit song "Single Ladies" [19] are few and far between. So while participatory surveillance as described by Albrechtslund might be empowering in that it helps to build online identity, the cultural context where it happens still needs to evolve so that the promises held by the concept of participatory surveillance can actually be realized.

Conclusion

I hope to have demonstrated that Internet surveillance is as multi-faceted as a solar-powered disco ball. The projects I have described above are participatory countersurveillance environments. They challenge forces that attempt to exert power through Internet surveillance. Those entities include (but are not limited to) governmental agencies, corporate (search engine) algorithms, as well as societal expectations more broadly. As an artist, it is my job to create environments where participatory countersurveillance can happen.

References

1. Anders Albrechtslund, "Social Networking as Participatory Surveillance," *First Monday* , accessed August 19, 2012, http://firstmonday.org/ojs/index.php/fm/article/view/2142/1949/

2. Albrechtslund, "Social Networking as Participatory Surveillance"

3. Sue Gardner, Knight Civic Media Conference 2013 documentation, accessed August 31, 2013, http://civic.mit.edu/conference2013/inside-out-whats-the-right--approach-to-change

4. Wikipedia contributors, "Algorithm," *Wikipedia, The Free Encyclopedia*, accessed August 31, 2013, http://en.wikipedia.org/wiki/Algorithm.

4. Christiane Schulzki-Haddouti, "Mit Google durchs WWW," Telepolis, February 27, 2001 (Hannover: Heise Verlag, 2001)

5. Annina Rüst, Documentation of TraceNoizer – Disinformation on Demand, accessed August 31 2013, http://anninaruest.com/a/tracenoizer/index.htm

6. Andrew McCallum, *Rainbow* , accessed August 31 2013 http://www.cs.cmu.edu/~mccallum/bow/rainbow/

7. Schweizerische Eidgenossenschaft, *Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)*, accessed August 31 2013, http://www.admin.ch/opc/de/classified-compilation/20002506/index.html

8. Johannes Korge, "Kampf gegen den Terror: SPD fordert Gesetz zur Vorratsdatenspeicherung," Spiegel Online, May 2, 2011, accessed September 7, 2013, http://www.spiegel.de/politik/deutschland/kampf-gegen-terror-spd-fordert-gesetz-zur-vorratsdatenspeicherung-a-760163.html

9. Prof. Dr. Dr. h.c. Hans-Jörg Albrecht, Dr. Phillip Brunst , Dr. Els De Busser, Dr. Volker Grundies, Dr. Michael Kilchling , Dr. Johanna Rinceanu, LL.M. , Brigitte Kenzel, Nina Nikolova, Sophie Rotino, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? (Freiburg: Max Planck Institut für ausländisches und interntionales Strafrecht, 2011)

10. Annina Rüst, Documentation of SuPerVillainizer – Conspiracy Client, accessed August 31 2013, http://anninaruest.com/a/supervillainizer/index.html

11. Annina Rüst, Documentation of *Sinister Social Network,* accessed August 31 2013, http://anninaruest.com/a/sinister-network/index.html

12. Jeff Baumes, Mark Goldberg, Malik Magdon-Ismail, and William Wallace, "Discovering Hidden Groups in Communication Networks", 2nd NSF/NIJ Symposium on Intelligence and Security Informatics (ISI 04) Tuscon, AZ, 11 – 12 June 2004, www.cs.rpi.edu/~goldberg/publications/hidden-graph.pdf, 1

13. William Bogard, *The Simulation of Surveillance: Hypercontrol in Telematic Societies* (Cambridge: Cambridge University Press, 1996), 27.

14. Albrechtslund, "Social Networking as Participatory Surveillance"

15. Amy Alexander, Annina Rüst, *Discotrope: The Secret Nightlife of Solar Cells*, accessed August 31, 2013, http://discotrope.org/

16. Thomas Edison, Annabelle –Serpentine Dance. Accessed September 27, 2013. http://www.youtube.com/watch?v=sNXNfcEo5dQ

17. Theresa Rizzo, "YouTube: The Cinema of Attrac-tions". Scan journal of media arts culture. Accessed September 27, 2013. http://scan.net.au/scan/journal/display.php?journal_id=109

18. FunnyDancingTV, *Fat Man Dancing to Beyonce.* Accessed September 27, 2013. https://www.youtube.com/watch?v=p-67Xt5R8DY

Acknowledgements

Thanks to Dr. Valentina Cardo, Lara Matta, and Dr. Catherine Sender for providing feedback on this paper. Many thanks also to my Discotrope collaborator Amy Alexander.

Author Biography

Annina Rüst produces electronic objects and software art. She creates technologies that are artistically and socially motivated. Her projects happen at the intersection of activism, algorithm, data, electricity, humor, politics, and pop culture. Her work has been reviewed in publications such as Wired and the New York Times Magazine. The Huffington Post called her recent robotics work a "Badass Feminist Robot". Annina's projects have been shown internationally in galleries, museums, and festivals such as Zero1 Biennial and Critical Make, as well as at the Edith Russ Haus for Media Art in Oldenburg, Germany. In 2014, she received an Art+Technology Lab grant from the Los Angeles County Museum of Art (LACMA). She has a Diploma from the University of the Arts in Zürich, an MFA from UC San Diego, and an MS from the MIT Media Lab. Annina has worked at Syracuse University since 2009. She has worked at Syracuse as Assistant Professor since 2009.