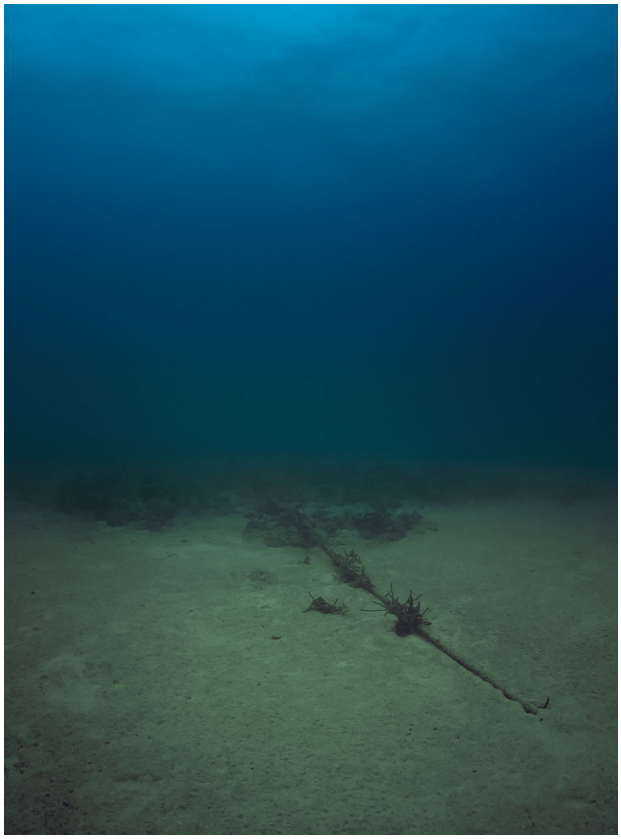
"Trevor Paglen and Jacob Applebaum," *BombMagazine.org* (Spring 2016).

BOMB



*Bahamas Internet Cable System (BICS-1), NSA/GCHQ-Tapped Undersea Cable, Atlantic Ocean*, 2015.

The following conversation is a transcribed and condensed version of a videoconference between Trevor Paglen in New York and Jacob Appelbaum in Munich. The exchange took place before audiences in both locations and was hosted by the NYC Goethe-Institut this past December as part of their symposium Images of Surveillance: The Politics, Economics, and Aesthetics of Surveillance Societies. It brought together artists, philosophers, writers, activists, and scholars, and opened Sensitive Data, a series of events that the organizers describe as "a long-term project that aims to advance international, interdisciplinary, and theoretical discourse and artistic exploration on and around surveillance and data capitalism."

Artist and geographer Trevor Paglen, renowned for his photographs, films, installations, lectures, and books on the theme of surveillance, engaged in a conversation with long-time collaborator, computer-security expert, activist, and hacker Jacob Appelbaum, who has contributed to the causes of WikiLeaks and Edward Snowden. They advocate for Tor, the global, volunteer-run, peer-to-peer anonymity network that is a viable alternative to submitting to ever-increasing mass surveillance. The images that appear throughout partly correspond to the works presented during the videoconference.

**Trevor Paglen:** We've come to learn that the network is hostile. The Internet was supposed to be the greatest tool of global communications and means of sharing knowledge in human history. And it is. But it has also become the most effective instrument of mass surveillance and potentially one of the greatest instruments of totalitarianism in the history of the world.

*National Security Agency, Ft. Meade, Maryland*, 2013.

**Jacob Appelbaum:** You might think of the Internet as a series of servers or companies and think of how you personally connect to it. Instead, there are signals intelligence stations around the world, along with enormous fiber-optic cables used for interception. Many computers have been compromised to serve for signals intelligence collection. Berlin and Vienna, for example, are signals intelligence platforms, which are actually used as part of the special collections service. When German Chancellor Angela Merkel was collected on by the NSA, it happened from a US embassy. In fact, we know that it happened from the one in Berlin, on Pariser Platz. The way that computers are broken into is via passive tap, a fiber tap of the kind that Trevor is fond of scuba diving for and taking photographs of. The collection is possible because the NSA works to compromise standards: you think that something is secure—you do banking online or read online—and the NSA makes sure that you believe it is safe, but, actually, it isn't.

Before Edward Snowden, when people said such things, the reaction was, "Oh, crazy conspiracy theorists." Now we know they were and are right. And that is not reassuring! We can now imagine this type of mass surveillance—all data being stored in a database—and what that allows for is a kind of time travel, if you will. When an intelligence analyst thinks you're interesting, they can basically travel back in time and see the things you've previously done and then decide if that is worthy of more inspection. That inspection will potentially include all of your web browsing or surveillance of all your telephone's content, as well as the metadata.

The program group that bothers me the most is called JTRIG [Joint Threat Research Intelligence Group] and they're a division of the British GCHQ [Government Communications Headquarters]. JTRIG is a mass propaganda operation; it's using data for disinformation and for changing political outcomes, harassing people, defaming and harming them—treating them as subhuman, effectively. And that's an entire division of the intelligence service; they have lots of people working on that. For example, they find someone who's a particularly religious Catholic or Muslim—I'm sure it doesn't happen to Catholics as much as it happens to Muslims—and then they use that information to blackmail them. These are the claims that they make themselves. They use the mass surveillance data sets—those fiber-optic cables—and there's a full life cycle between the cable tap and actually using that information to harm people in a material fashion. For me, that's the hallmark of a tyrannical operation. I don't want to see governments engaged in those kinds of secret and damaging activities.

*National Security Agency Utah Data Center, Bluffdale*, UT, 2012.

**TP:** One way the network is hostile is that state actors are conducting mass surveillance and are attacking critical infrastructure using weaponized malware. They orchestrate propaganda and blackmail operations against political enemies. There's another side of the hostile network, which is done by corporations. We all know for a fact that Google and Facebook are collecting enormous amounts of data on every single person who uses their services and they are conducting analytics on a scale that was unimaginable even a few years ago: tracking everybody who uses credit cards, who uses a cell phone, and so forth, and collecting intimate details about their lives. Google probably knows more about me than my family does.

Today, in large part, that information is being used to sell you things, or they try to sell your information to advertisers. But tomorrow, that information will be used in all kinds of other ways. We can imagine your Google searches modulating your credit score, we can imagine a picture of you drinking a beer that you posted on Facebook will be recognized by an object-recognition algorithm. Maybe Facebook will want to sell that to your auto-insurance company, and your auto-insurance company would change your insurance rates based on that. We can imagine that if you wear an exercise-monitoring device like Fitbit, corporations will be collecting intimate vital metric data on you. If you don't exercise, maybe your health insurance premiums go up, and if you do exercise, they go down.

But the point is that—although it's not evenly distributed yet, this will increasingly be true in the future—the rights and the

Still from *89 Landscapes*, 2015.

privileges that you have will be modulated according to these kinds of metrics. In China this is already beginning to happen.

**JA:** The Chinese scoring system is part of their identity intelligence—these guys are all about doing everything they can to identify everybody in every way. The scary part about what's happening in China is how we can imagine it as the future everywhere. Identification of all things at all times and their correlation and linking with data sets effectively means that there's a database of all of a person's activities linked through time with their identity and anything that might identify them—their fingerprints, their biometric passport, their retinal scans, and whatever else is going on.

Imagine big data analytics processing your personal patterns—biometric, biographic, contextual, what you read, your military service, whatever it is that you might do. This might include your social relations: you have a friend who smokes, and his or her credit score goes down. Then your credit score also goes down because you keep the company of someone who smokes. It's a paternalistic control and surveillance that informs automatically. You no longer need people to tell on each other. The mere existence of certain devices ensures that the devices themselves tell automatically. This is the nightmare of the science-fiction writer Philip K. Dick. Not that everyone would be a spy—that's sort of a trope about the former East Germany—but that every thing would be a spy … I think it's in Ubik, there's a doorknob which is a sort of Internet of Things doorknob. When someone wants to open the door, the doorknob demands to be paid. And of course the person says, "I don't have to pay you." And it says, "Well, actually if you look at the contract you signed when you took this doorknob, you'll find that, in fact, payment of the doorknob is a necessity if you wish for it to open the door."

We're sort of moving into that world. While it doesn't seem so obvious, if you look, you see patterns emerging about social control in which you want to have those doorknobs to track who might be opening the doors and whether or not you want them to open. I mean, it's really an extreme of the control society tied directly to your identity.

And there are in fact plans for something called real-time tipping. The NSA will ensure that if you ride on a train or a bus or fly on an airplane, you'll have to show an identification card even for domestic travel. And it's tied to biometric information. In other words, you scan your Lufthansa boarding pass to fly from Amsterdam to Munich, as I just did today, and a real-time alert that I was traveling would be sent to an analyst or to a database. And if someone decided that I was a person of interest, I would get tipped off and sent to an analyst in real time. And now you start to see how these things tie together—it becomes extremely alarming to think about how this information might be used to impact your life. It's a very scary thing.

The system might also work in your favor when you behave well. You buy the right brand of thing, which needs to be bought today because the centrally planned economy says so, and you may get VIP treatment at the airport. You get a high score and preferential treatment because you're leading the way by doing your civic duty and it's automatically "told" that that's the case.

Trevor and I are not futurists when we talk about this. This is a present thing. It just isn't entirely clear yet how and when it works and how it is in fact doing this. The Chinese, weirdly to their credit, are actually completely open about it. It took Edward Snowden for us to learn that the NSA has the same plan. When you fall into the bad credit score in the NSA system and you happen to be a twelve-year old Muslim in Pakistan, you get droned.

**TP:** The Internet is a predatory network that is, on one side, potentially a very coercive tool of totalitarian power and, on the other side, a tool that will increasingly be used to allocate rights and privileges through commercial means—credit scores or insurance rates and that sort of thing. Given that situation, can we imagine a different kind of network? Can we envision a network that is nonhostile? Our project Autonomy Cube is an attempt to imagine what this alternative network might be like.

This is the sculpture that we made. There are a couple of them around the world now. You put the sculpture in a museum or a Kunsthalle or what-have-you and it sits on the host institution's Internet connection. You plug it right into their Internet. And once you've done that, it does a couple of things. First, it creates an open Wi-Fi network throughout the museum for anybody to use. Then it routes all the traffic over the Tor network. Tor encrypts the data, which results in a more secure Internet using the host institution's Internet connection. The other thing that it does: it turns the museum into a Tor relay, making it a part of the Tor network's infrastructure.

Jacob Appelbaum and Trevor Paglen, *Autonomy Cube*, 2015.

**JA:** The Autonomy Cube has a feature that is very uncommon here in Germany and I'm not sure about New York City these days—the Wi-Fi connection is one where you don't need a password at all. The reason is that when you join the wireless network, you actually route, not through the normal Internet connection, but through Tor, which means that what you do there does not trace back to the museum but to the Tor network instead.

It's a peer-to-peer network and the sculpture is itself one of the peers. When you use this network it allows you, for example, to pop out in Russia or to pop out in the Netherlands or to go through the United States. The websites you might visit—or your email provider when you check your mail—they'll see you not as coming from wherever the sculpture is installed but as coming from this other place. If you've ever seen a bad Hollywood movie where they try to trace hackers around the world, it's like that—except the users can't be traced, which is kinda nice.

*National Security Agency Surveillance Base, Bude, Cornwall, UK*, 2014.

The actual Tor relays are run by volunteers around the world and we need more of them. Because this is a so-called overlay network, you have to have a network on top of the network to be able to get certain privacy and security properties that can hide your metadata. There's a huge discussion about hiding content versus metadata these days, especially with data retention. Data retention is a concept that allows the collection of enough information to know a great deal about you, even if you were to encrypt the contents of your message. So if you go to your bank every day to check your bank account, they would probably know that it's you that went to a certain bank. Using Tor, they would see someone from the Tor network has gone to that bank. That's a big difference. When you look up medical information, for example, with Tor, somebody somewhere knows that someone looked that up, but they don't know that it was you.

So the Tor relay in the museum is not about helping people in the museum—it's about helping everyone else to enjoy the freedoms that the museum brings, but from any point in the world. So everyone who uses Tor right now has a probabilistic chance of routing through our Tor relay in Oldenburg. There are Tor relays in the Reina Sofía Museum in Madrid, at Metro Pictures in New York City, and at the Witte de With in Rotterdam. The museum is a bastion of free speech, helping to protect everyone's right to read and speak freely on the Internet, even if they're not in the museum. So the museum becomes a part of the infrastructure of fundamental liberties. There are many people all around the world who need this privacy-preserving technology. With Tor, you have the ability to look at the source code that makes up the program; you can modify it, share modifications with other people, and run it for any purpose. Those are the four freedoms of free software. You can download the software to your computer when you leave the museum and continue using it. You can put it on your phone, on your mobile computer, wherever you want. This is not just imagining a new future, it's actually building that alternative future as we speak—and you can use it right now, wherever you are in the world.

**TP:** I'm thinking about the ways in which we are talking to artists from the past when making artworks—while also talking to people in the present. Our project is very much influenced by post-Minimalist sculpture, especially Hans Haacke and his Condensation Cube. It's combining what's sometimes called Systems Art with Institutional Critique.

There's a whole history of artists engaging with Institutional Critique, looking at the guts of the exhibition places where they will be showing work. An artist might look at the funding structure of the institution, uncovering a museum's financial politics, which are also the politics of the collection. It's a critical tradition in art to pull back the walls and to see how the guts of the institution work. We're inspired by these investigations into the infrastructure, politics, and economies of museums, but we are approaching them in less critical ways and more in terms of enhancement.

Still from *89 Landscapes*, 2015.

The Autonomy Cube is a way of enhancing museums—for a couple of reasons. Right now, institutions are almost on autopilot trying to install more and more invasive surveillance systems. They are unthinkingly installing biometric surveillance setups, which track how people move around in a particular space. You can imagine why a department store would want to do this: they want to know what displays are the most successful, what's the best architecture for selling different kinds of products. But increasingly, civic institutions like museums are also installing these types of systems that track people's faces, that track the artworks which people are looking at. And one can understand why they would want to collect this demographic data to do their own analytics, to use in fundraising, and that sort of thing. But what we're proposing is that civic institutions and museums should perhaps do the exact opposite: they should be the bubbles in society that are free from this type of data collection.

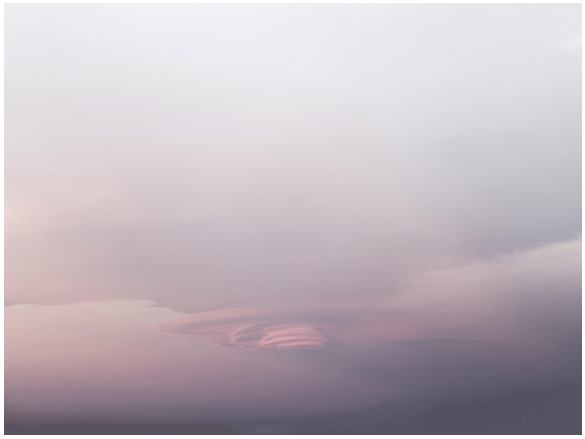
And this goes back to a very old idea in democracy, which is that you need to have certain institutions that allow for freedom of exploration and freedom of expression. I want to give a shout-out here to Alison Macrina from the Library Freedom Project. Alison has a project that's analogous to ours in that she's using installments or relays in libraries, which are fundamental democratic institutions where you can go and explore any ideas you wish to learn about. They provide an enormous amount of intellectual freedom. Free libraries foster a society where you have an educated populace and diversities of opinions. But the other very important thing about libraries is that the police don't get a record of the books that you check out. In other words, you are able to use a library to explore culture and information anonymously. And that anonymity is a crucial part of the freedom and the contribution to a democratic society that a library affords.

Our proposal is that museums should do the same. They should be places where you can go and encounter ideas that might be challenging, where you are given permission to look at images and think about concepts that you don't always have permission to think about in your everyday life. We propose to approach museums as safe spaces from a world that is increasingly tracking everything you do and collecting as much information as possible about you. The proposals that we're making with Autonomy Cube, with the Tor network, and in our exhibition and lecture projects are aimed at the future of civic institutions in general.

Every time we talk about our work, people say, "But what about the Internet apocalypse? What if people use the Tor network to do bad stuff?" Jake, do you want to take that on?

Still from *89 Landscapes*, 2015.

**JA:** Oh, you could answer that, Trevor. (laughter) First I want to echo what you just said: the Library Freedom Project is really important. Alison is the Emma Goldman, I would say, of anonymity in the modern world. She travels all around the globe and teaches people about anonymity. And she faces the same questions. The front-runners of the "info apocalypses," as people like to call them, are essentially child pornographers, drug dealers, terrorists, and money launderers. You always hear that the reason you can't actually have any civil liberty on the Internet is because of these four groups. It is the case, of course, that the Tor network is a reflection of the larger Internet and there are people who might buy a weapon online using Tor. This is, of course, very regrettable. But there's a big difference in scale, which is often lost: the majority of weapons are not being traded on the Tor network or on other anonymity systems.



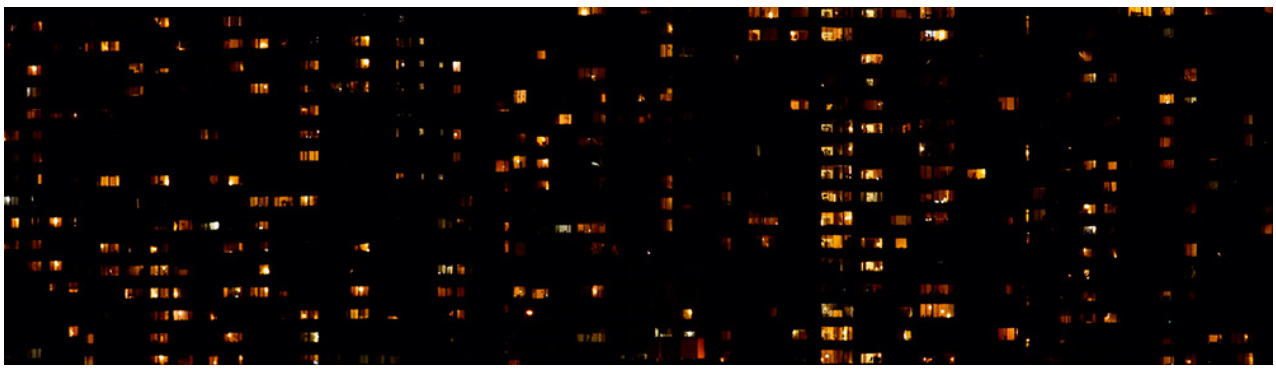
*Untitled (Reaper Drone)*, 2013.

The same happens with other criminal activities. While it is true that you can find child pornography on the Internet, it's also true that the police who investigate the crime need the protection of networks like Tor in order to hunt down the perpetrators. So if you give people this anonymity they will use it, in theory, to do very good things and also clearly very bad things. Someone downloading information about drugs may be a person exploring, or it may be police officers gathering evidence. So in general, we have a counterintuitive situation here: we might want to shut down every avenue for terrorists to have a conversation. But if we cut off all the avenues of speech, we haven't stopped those people from existing. We have merely blocked off our ability to spy on them and to understand what they are saying.

Of course, Tor won't be able to stop people who have the desire and the ability to break a law and are willing to commit heinous crimes like terrorism or large-scale money laundering like HSBC did and get away with it, or child pornography. On the flipside, if we take away Tor, we are left without an option.

In other words, Tor is the option for law-abiding, reasonable people—even if it's sometimes used by police officers who commit acts of police brutality against civilians when it is a crime to do so, or by American soldiers who commit war crimes, and even by regrettable people like child pornographers, terrorists, and drug dealers, you name it. But it's really hard to design a system where, for example, the Chinese idea of the bad guy, or the German or the American idea of the bad guy, would be stopped. And what would happen when you have built in such a facility? Then it would become even clearer that the people who built and run the system are even more at risk than they were before, because they're in a position of power.

So the idea instead is to increase everyone's liberty and to give regular people an option that doesn't cost them money and is helpful in the sense that they are now more protected. Meaning that their rights are now larger than they were before. This is very important for not only resisting censorship of certain things, but also for making sure that there isn't mass data collection that's tied to you for the rest of your life and that becomes a function of wealth and privilege. With Tor, you'd be able to have some sort of privacy.

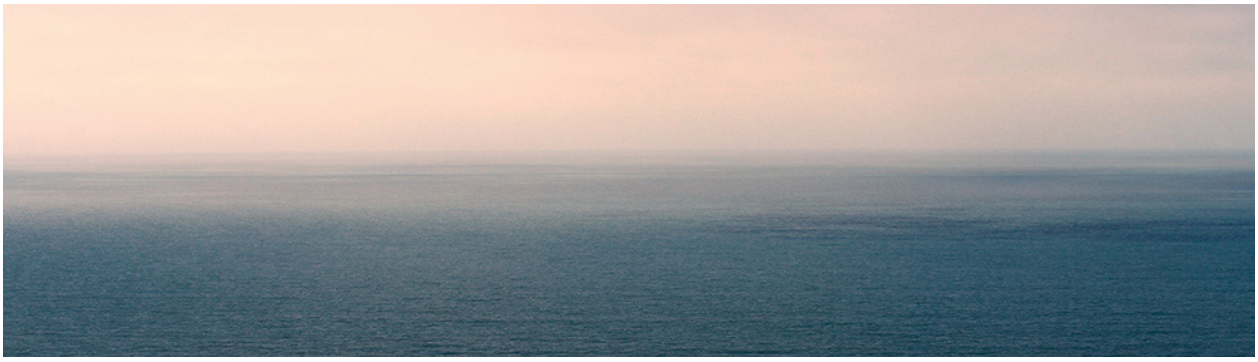


Still from *89 Landscapes*, 2015.

**TP:** The point is that Tor saves lives. If you are queer and young in Uganda and you want to connect with other people like you around the world and you do that on the normal Internet, you are putting your life at risk. If you're an activist in Iran or Bahrain or Saudi Arabia, Tor will save your life quite literally if you want to communicate with the outside world. If you are in China, or in Turkey for that matter, and you want to circumvent the state censorship that happens there, Tor allows you to communicate with the rest of the world in a way that is more secure than using the hostile network. Or, if you are a mom in the United States and you want to understand more about your kid's health problems and don't want to give that data to Google or to Facebook, you can use Tor to protect your information.

Both Jake and I believe that we are not going to engineer our way out of a totalitarian future. Technology won't save us. Tor will not save us, but it can help. What this project is about is trying to show the ways in which technologies congeal social, political, economic, and cultural relationships. Let's think about what technologies and communication infrastructures may look like if we try to build them with different values at their core. We imagine an alternative to the hostile network that is preying upon us all the time, and try to enhance the parts of the network that do allow us the kinds of freedom and intellectual exploration and participation in democratic projects that were previously unavailable to us. In other words, can we reimagine the promise of the Internet toward a more productive future?

**JA:** I would add that there are different stages. We can imagine that we would protest certain things because we don't like them. The reason for resisting is not because you think that you're going to win, but because you know that it is the correct thing to do. And that is not an easy thing to say. I doubt that we will see the end of mass surveillance anytime soon. We won't win it in our lifetime. But we must resist because it is in fact something that we do not want. We even wish that we had not been born into this situation. So we should return with some efforts to change that the situation. And this project goes beyond resistance by building an alternative. It is real and it is the best thing that we have. Part of what we want to do is to inspire other people past the security nihilism that brings us into a passive place where we don't critique the system anymore because we feel disempowered, where we don't speak because mass surveillance silences us, where we say there's nothing to be done because technology alienates us. If we can imagine something different, we might participate in another way. In fact, we could build a different world.



Still from *89 Landscapes*, 2015.