Digital War
https://doi.org/10.1057/s42984-021-00036-z

INTERVIEW

Interview with Paolo Cirio

Chin-chin Yap[1] · **Paolo Cirio**[2]

Accepted: 10 September 2021

Introduction

Paolo Cirio is one of the most innovative artists working at the intersection of art, technology and activism. Cirio, often described as a hacktivist, uses various forms of technology such as artificial intelligence, facial recognition, data harvesting and mining to highlight socio-political injustices and state and corporate abuses of power. His works examine the structures of capitalism and globalization, matrixes of online production and consumption, and how technology is transforming notions of privacy and personal identity. Some works are presented as satirical websites appropriating existing platforms in which the public can participate.

Cirio's most prescient and provocative works expose the privacy risks and psychologically manipulative tactics underpinning the billion-dollar social media industry, showing how users are constantly nudged into generating content and exposing personal information that is relentlessly exploited for corporate gain. In *Face to Facebook* (2011), Cirio used artificial intelligence to re-purpose 250,000 Facebook profile photos for a fake dating site where one could search for a significant other based on certain characteristics associated with their photo. Similarly, Cirio harvested one million Twitter users' publicly available metadata for *Persecuting US* (2012) and assigned them political affiliations on a custom-made website based on their public statements and social connections. For the project *Street Ghosts* (2012–2017), he found publicly available photos of people on Google Street View and pasted their life-size, color versions on building walls at the actual physical locations as indicated by Google.

While most consumers are aware that there are privacy risks associated with the use of everyday technology and social media, Cirio's interventions demonstrate the logical extremes of online exposure in ways that are both satirical and shocking. His works make evident the dangerous ease with which personal information can be not only obtained but misused.

Cirio's latest work to make the headlines is *Capture* (2020), a database of 4000 photos of French police officers identified by name. Cirio had obtained the photographs, which were taken at protests or other public events, online and from journalists. He presented them on a custom-made website, capture-police.com, where visitors were invited to identify the officers. The work is a response to deployment of facial recognition by the French police, which after his work also pushed for a controversial French bill seeking to criminalize the publication of images of on-duty police officers with "intent to harm their physical or psychological integrity." Across France, tens of thousands protested against the bill, known as the 'global security bill,' and media and human rights organizations warned that the bill would suppress press freedom and decrease police accountability for the unlawful use of force. *Capture* was intended to premiere at the Le Fresnoy – Studio national des art contemporains in Tourcoing, France. When Cirio announced the project on Twitter on October 1, 2020, Gerald Darmanin, the French Minister of the Interior, tweeted: "Paolo Cirio: An unbearable lynching of women and men who risk their lives to protect us. Unless 'the exhibition' is called off and all the photos removed, I will bring the case to court." *Capture*'s French premiere was cancelled.

On April 14, 2021, the French National Assembly passed the amended bill by 75 to 33 votes. The bill states: "Causing the identification of an officer of the national police, a member of the national gendarmerie or an officer of the municipal police when they are taking part in a police operation, with the manifest aim of harming their physical or psychological integrity, is punishable by five years in prison and a fine of 75,000 euros."

Cirio's works have been internationally exhibited in institutions including Vienna's Kunsthalle Wien and London's Tate Modern and Victoria and Albert Museum. He has been

✉ Chin-chin Yap
chinchinyap@gmail.com

[1] Lisbon, Portugal

[2] New York, USA

Published online: 05 November 2021

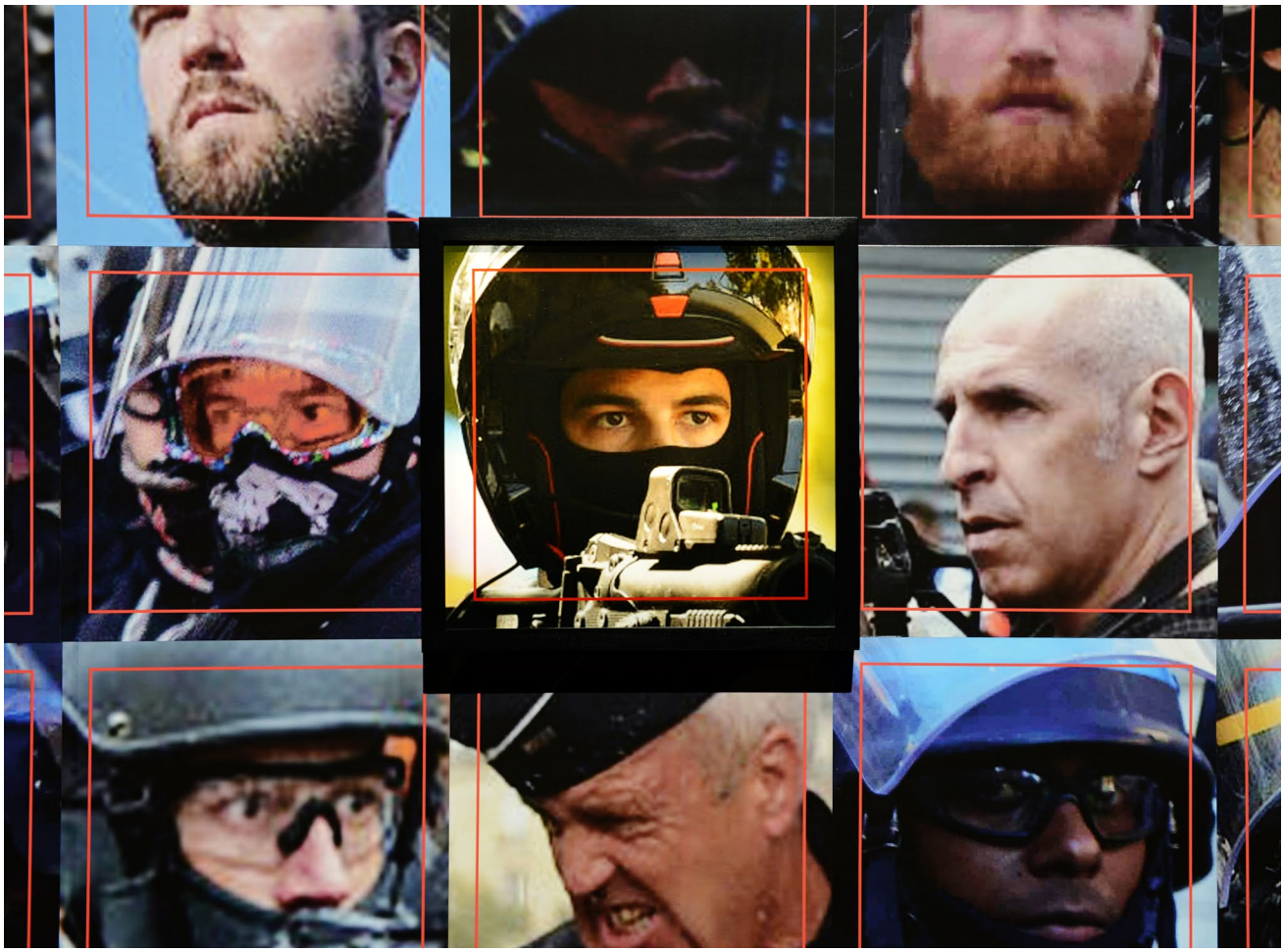

IMAGE 1: Paolo Cirio, *Capture* (2020), detail. C-prints and inkjet prints. Copyright Paolo Cirio.

featured in major exhibitions including the Gwangju Biennale (2017) and Sydney Biennale (2007), and won prizes including the Golden Nica first prize at Ars Electronica (2014) and second prize at Transmediale (2006).

Interview

CY: You use strategies of creative resistance to expose abuses of power, particularly by corporations and states. But your work is also very special in your attentiveness to the individual and the opportunities you provide for democratic participation. This seems to restore some agency to the individual, even if it is largely symbolic. The concept of digital war is something that recurs powerfully in your work, although we might not usually use the terminology of war to refer to these subjects. Traditionally, war is declared by governments, but now there are so many wars by other names. Cybercrime, surveillance, and technologies of commodification and oppression are expanding in scope and scale. There are wars inflicted by governments and the military-industrial complex that are only possible because of digital technology.

The geographer Derek Gregory introduced the concept of a 'battlespace' that has sublimated our conventional notions of warfare. Instead of traditional battlefields where two parties declare war upon each other, ordinary citizens now live within a world that has become a battlespace of many dimensions. Here, states and corporations are constantly, relentlessly commodifying individuals and exploiting them for profit. They do this with such craftiness that ordinary people may not even know they are caught in this battlespace even as their lives are shaped by it. Naturally, technology and social media play a huge role in this digital war. Your works go beyond pointing out the consumerism and digitization of contemporary life. They

demonstrate how successfully global capitalism has co-opted us into Debord's 'society of the spectacle.' as a profit-making strategy. Could you tell us how your artistic trajectory developed in this direction?

PC: I was politically engaged from a young age. Since I was very young, I felt moved to express myself and do something in this world. I grew up in a very remote part of the Italian countryside. My parents were farmers and at the time we were very isolated from 'culture.' At the same time I was a very active and curious child, so the internet was a way to connect to the world and a place where I could voice my thoughts and opinions. The more I learnt about the internet, the deeper I went down its rabbit hole. Nobody really knew what the internet was about in my region, at the end of the 1990s, but to me it was clear that it was going to change everything. Basically, I'm self-taught. To be a hacker you need to spend nights and days in front of the computer and learn techniques to break a system, things they don't teach you in school. Even as a minor I went to hacker meetings as there was a hacker scene in Italy, and then I travelled to Amsterdam and to Berlin where the scene is much bigger. Europe is very politically dynamic and there was fertile ground for such activities.

Since the beginning of the anti-globalization movement, I was involved with social movements, in particular the anti-war movement just after September 11 and all the wars that followed. I started to be active in hacktivism against NATO, which at that time was the main target of anti-war movements in Europe. I was doing research and organizing DDoS (distributed denial-of-service) attacks that are now very common, but weren't back then. I was also part of the first bloc of people who published information from alternative sources on the internet. Of course, this is now an everyday affair, but back then it was quite revolutionary to use technology as a weapon, so to speak, in this manner. The internet started as a military project and then it expanded into all facets of life. The digital economy has come to monopolize content and politics and it's changed actual political processes; we saw this very clearly with Trump. Now, we've reached a point where every person has a computer in their pocket, so the internet affects each person on a very personal level. So, the notion of cyberwar began in the military, and now it's in every sphere of our lives: economic, legal, political, and personal. We're used to seeing one country waging war against another, but here it's a multilateral war where everyone is pitted against each other without much coordination.

CY: How do you see digital war materializing in politics, culture, and economic matters? For example, one can be dramatically assassinated by a drone, but we also have many everyday 'deaths by a thousand cuts' that go unnoticed. The migration crisis, for example, is one of the world's most pressing problems and it's brought about in part by digital weaponry. Many refugees are direct victims of the military-industrial complex's insatiable hunger for war profits; others are indirect victims of extractive capitalist tools such as financial and technological systems. If they make it to Europe or America to seek asylum, they're also subjected to various profiling systems. It's as if they're trapped in ongoing facets of a digital war.

PC: Indeed, there are many realms of digital war and just looking at technology alone is reductive. I talked about this in a text from 2019 called *The Flowchart*, where I describe the flows of information and operations that make up our interconnected world. In contemporary society, there are flows of money, goods, people, media, images, information, and even environments, laws and intellectual property. These flowcharts give us a more accurate idea of globalization's character and how instruments of power function.

The use of technology in migration flows is definitely an important issue. Apart from the policing and militarization of borders, how do you use identification systems with regard to undocumented crossings? States should use border controls or tracking but not military tools; this is not a military issue. Even if states possess the most advanced technology that might be useful in a war zone, context is important; these tools should not be deployed against citizens or civilians. However, the EU's 'security-industrial complex' leads to the promotion, defense and increased use of securitisation technologies.

During my research, I found a number of EU-funded projects that are used to police borders in ways that overstep human rights. Three of them are SPIRIT, iBorderCtrl and Prum System. The Europol and Frontex agencies already use advanced biometric technology to survey borders and profile travelers. SPIRIT is an EU Horizon 2020-funded project to scrape social media images of faces to build a database for facial recognition analysis. Five law enforcement-related stakeholders are involved: Greece's Hellenic Police, the U.K.'s West Midlands

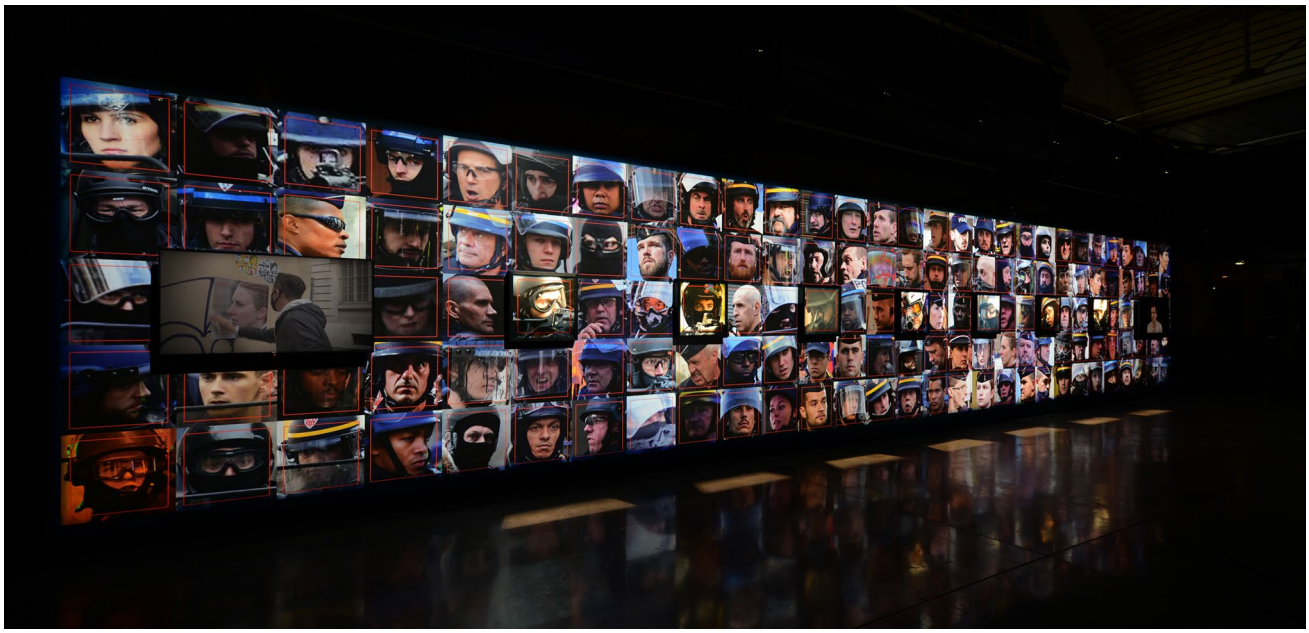

IMAGE 3: Paolo Cirio, *Capture* (2020), installation view at Le Fresnoy – Studio national des arts contemporains, Tourcoing, France. C-prints and inkjet prints. Copyright Paolo Cirio.

Police and Police and Crime Commissioner for Thames Valley, Serbia's Ministry of the Interior and the Polish Police Academy in Szczytno. The project aims to use tools such as face extraction and matching from social media data in a way similar to that of the U.S. company Clearview AI. iBorderCtrl is a European-funded research project on biometric data seeking to deploy "lie detectors" for refugees seeking to enter the EU via the Hungarian, Greek, and Latvian borders. Lastly, the Prum System is an EU-wide initiative connecting DNA, fingerprint, and vehicle registration databases for mutual searching. Ten European member states, led by Austria, want to create a network of interconnected national police facial recognition databases spanning the whole of Europe and the U.S.

Furthermore, Amnesty International found that three companies based in France, Sweden and the Netherlands have sold digital surveillance systems including facial recognition technology and network cameras to key players involved in mass surveillance in China. In some cases, the exports were directly for use in China's indiscriminate surveillance programs which may target Uyghurs and other predominantly Muslim ethnic groups throughout the country.

In some countries such as India, ordinary citizens can't move through the country or even access water without the right identification. Now, they're using an iris scan to create a unique biometric ID to access services. I don't agree with the push to use biometric ID as there are other technologies that are simpler and safer. Of course, there are design issues involved with any technological innovations, and therefore, it's important that the designs are developed in the right way and that any negative or discriminatory consequences are properly considered.

CY: Your most recent work *Capture* (2020) used facial recognition technology to construct a database of 4000 French police officers identified by name. Its French premiere was cancelled by Gerald Darmanin, the French Minister of the Interior, and you received legal threats and even death threats. Could you explain your idea behind this project and how it evolved from your body of work?

PC: Actually, I first started using facial recognition technology in *Face to Facebook*, a project presented in 2011 which I'd been developing for a couple of years. I scraped Facebook for one million publicly available photographs of faces and used artificial intelligence to sort them according to their expressions. Then, I created a fake dating site called lovely-faces.com using 250,000 of these photos where people could search for their significant others using certain filtering criteria for emotions and personality traits.

CY: As you stated on the project website, Facebook has created a "naturally addictive" form of social

networking which in fact creates a completely new form of online identity. Facebook's business model is based upon manipulating user psychology to maximize online participation in "induced immaterial labour with instant gratification." The interesting part is where these facial recognition techniques are applied not to identify suspects or criminals but to "capture a group of people with similar somatic experiences," so that "different elements forming the identities can be remixed, re-contextualized and re-used at will."

PC: *Face to Facebook* was a very provocative and widely covered project that caused me to receive threats of legal action and even death threats. Now, ten years later, facial recognition technology and the use of machine learning to identify faces and expressions is very common. For *Capture*, the techniques were actually much simpler because in this case I didn't have to examine the expressions of these faces; I just had to literally capture those faces in photographs. It's actually not so high-tech. There's an algorithm behind the facial recognition technology but it's something that doesn't hurt anyone– just finding and cropping a face in a photograph.

The other part of the project consisted of creating a database of faces at capture-police.com where people could type the name of a police officer and associate the photo with a name. That's not technologically difficult; it could even be done with a spreadsheet, for example. However, the creation of the database itself is dangerous, which is the central issue in all these privacy wars. A technology may be able to automatically detect something – your face, your fingerprints, biometrics—but that particular unit of information is meaningless if it doesn't relate to a particular person. It becomes dangerous when it becomes a unique identifier that is biometric, or connected with a name, address, or a Facebook account that contains even more personal data. That's when the real privacy threat occurs. Once one set of associations is made, then we have to deal with another layer of privacy concerns– if these identifiers related to biometric data are public information, or how they stay private. There are many layers of complexity that can potentially make a particular unit or link of data a dangerous weapon. Technology is important but equally critical is how it's used or regulated so that it does not cause harm.

CY: Do we have any realistic hope that companies that control our personal information will treat it with privacy and respect, or even according to the law?

PC: That's a big question. Citizens can't do much unless they organize themselves in democratic institutions and are able to moderate speech in conjunction with surveillance, privacy and transparency concerns. Corporations have a huge role in these processes but they're economically incentivized to capture as much of our information as possible, so they brand themselves as the guardians of free speech while they actually have a huge role in manipulating our information. For example, search engines will offer results based on advertisers' interests without care for context or sensitive information.

In 2018, I developed a project called *Right to Remove*, at www.right2remove.us, which is a campaign and tool to help ordinary individuals remove sensitive information from the internet that produces online bullying or infringes on human dignity, such as slander, hate speech, and revenge porn. Many countries have introduced laws for the 'Right to be Forgotten,' but in many cases, they are not yet properly and swiftly implemented. Our social norms with regard to the internet are changing and we're still learning how to negotiate our personal freedoms in online communities. As I wrote in a text called *Perceptions on Systems of Justice Over the Internet,* human civilization is the constant process of negotiating laws and social culture that enables us to co-exist. For example, many religions teach us concepts of mercy and forgiveness, but you seldom see these concepts being practised online. Instead, we are still in a developing period where people feel empowered by meting out crude justice from behind their laptop screens. Currently, each country deals with these regulations with national laws. For example, in the U.S., facial recognition technology is even regulated by cities; it is banned in Boston, San Francisco and Portland. But that makes no sense because people move around the world and not only within a particular city in the U.S. There are a huge number of other issues about content moderation that are also connected to privacy. We don't really know what companies do with our personal data and how to hold them accountable when they operate worldwide. There are so many different layers of regulations and it's very difficult for ordinary citizens or consumers to know how information is being used.

New technology creates new opportunities for companies to capture value. These new types of assets aren't regulated by law, at least in the beginning, but once the genie is out of the bottle, it is hard to put it back in.

CY: There's a sizeable time lag between technological innovation and legal regulation.

PC: The gap is indeed quite large because technology is much faster than the law. But this is all new to humanity: we've never evolved so quickly before, with so much technological innovation at our disposal. If you look at humanity in the past few centuries, technology became an issue only a hundred years ago when computers and information technology enabled a much faster pace of innovation. This seems all new to us, but imagine where we'll be one or two hundred years from now. We are probably going to go through many wars where people will die. But we'll get to a point where we know how to deal with it. Right now we're like babies at war against each other trying to understand something much larger than ourselves. We don't speak the language; we don't have agency.

I know everyone says things are getting worse, but in my generation I saw great improvements. Ten years ago, it was even worse because we didn't even think about the need to regulate companies such as Facebook; today, everyone is aware of these dangers and there are laws concerning privacy and free speech everywhere. What we really need is for global organizations or agencies to take charge of some of these issues. Take the United Nations. We think it's a very old institution but it's actually very new and came out of two huge wars, huge disasters. We know what the Nazis did but think about the U.S. dropping an atomic weapon on Japan. The U.N. came out of that situation. At some point, the U.N. or another organization will step in and regulate technology in a similar way to nuclear weapons and genocides. There are still genocides happening but think about how much more equipped we are to tackle this problem. This is also a technique of war. Two hundred years ago, the strategy was to start a war and kill everyone. Invasions like that are now much rarer, comparatively speaking. As much as I can be negative, it's also important to have perspective. We need to keep fighting and speed up the change for good. Humanity and civilization is what it is but we can speed up its development and eventually less people will suffer.

CY: Are there any areas in our use of technology today where you see obvious red flags, such as unregulated moral and ethical issues?

PC: The list of ethical issues is quite long. First, there's a difference between ethics and morals in that morals tend to be fixed and ideological, whereas ethics are more dynamic and are constantly being shaped as social contracts. Artists play a central role in the shaping of ethics. In terms of the issues, free speech and privacy are definitely my main concerns. But it is also about our cultural understanding and representations of technology and related fields. This is where the work of artists is important when the media does not succeed and institutions manipulate our understanding of developments in finance, technology and politics. Artists can offer better visions with critical approaches and push the boundaries of reality by unveiling its potentials and dangers. This is also an important part of the digital war.

Facial recognition is a major issue because it can be used not only for surveillance but also to target individuals in warfare situations. Companies and governments have a huge interest in using this, and it is hard to stop them as this technology is very easy to develop and use. But in a few years, there's been so much debate about it, and proposals against it, so it is possible to ban. People can step in and fight against it; they'll eventually be heard by some concerned politicians, and some countries start to see the risks. China, for example, is one of few countries in the world where facial recognition is used without regulatory issues, which results in violations of human rights. Yet, negotiations with other countries can be effective, once facial recognition is considered a global thread, a weapon of mass destruction, also China and Russia can be persuaded to ban this technology. That's what I have been pushing for with projects such as *Capture*.

As a European, I was very surprised that facial recognition wasn't yet regulated in Europe. I started to collaborate with other privacy organizations to understand the ratifications of banning facial recognition through regulation—where it was used, why, and by whom. There wasn't much creativity per se there. It was a lot of research and activism that just concluded. In September 2020, I filed a petition, which you can see online at Ban-Facial-Recognition.EU, to permanently ban facial recog-

nition technology in Europe on the grounds that it violates fundamental human rights and misuses public funds. We had over 52,000 signatures and it was sent to several European agencies including the European Commission, European Parliament and the Council of Europe. It is not going to be easy but the European Union is considering banning facial recognition in all of Europe, which means it is not impossible.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1057/s42984-021-00036-z.

Chin-chin Yap is a writer and filmmaker specializing in art law and human rights. She produced the documentary films *Rohingya* (2020), *Ximei* (2019), *The Rest* (2019), and *Human Flow* (2017). Recently she edited the book *Human Flow: Stories from the Global Refugee Crisis* (2020) and has been published in *Art Asia Pacific*, The *Tax Lawyer*, and the *Columbia Journal of Law and the Arts*. She has a B.A. from Columbia University and a J.D. from Georgetown Law School.

Paolo Cirio is an artist working with legal, economic, and cultural systems of the information society. His artistic research and interventions take the form of photos, installations, videos and public art. His work has been internationally exhibited in museums including Vienna's Kunsthalle Wien and London's Tate Modern and the Victoria and Albert Museum, as well as the Gwangju Biennale and Sydney Biennale. He has won numerous prizes including the Golden Nica first prize at Ars Electronica in 2014 and second prize at Transmediale in 2006.