GRIPPING, VITAL READING, EXPLAINING HOW CORPORATE AND GOVERNMENT CONTROL OF THE INTERNET POSES A FUNDAMENTAL THREAT TO OUR FREEDOM AND DEMOCRACY
— OLIVER STONE

AN IMPORTANT WAKE-UP CALL ABOUT A POSSIBLE DYSTOPIAN FUTURE, WHICH IS A TECHNOLOGICAL REALITY NOW
— NAOMI WOLF

OBLIGATORY READING FOR EVERYONE INTERESTED IN THE REALITY OF OUR FREEDOMS
— SLAVOJ ŽIŽEK

THIS BOOK BREAKS A SILENCE IT MARKS AN INSURRECTION OF SUBJUGATED KNOWLEDGE THAT IS A WARNING TO ALL
— JOHN PILGER

OR Books
www.orbooks.com

CYPHERPUNKS

ANONYMOUS

JULIAN ASSANGE

with JACOB APPELBAUM ANDY MÜLLER-MAGUHN
and JÉRÉMIE ZIMMERMANN
CONTENTS

INTRODUCTION: A CALL TO CRYPTOGRAPHIC ARMS 1
DISCUSSION PARTICIPANTS 7
EDITOR’S NOTE 11
NOTE ON THE VARIOUS ATTEMPTS TO PERSECUTE WIKILEAKS AND PEOPLE ASSOCIATED WITH IT 13
INCREASED COMMUNICATION VERSUS INCREASED SURVEILLANCE 21
THE MILITARIZATION OF CYBERSPACE 33
FIGHTING TOTAL SURVEILLANCE WITH THE LAWS OF MAN 41
PRIVATE SECTOR SPYING 51
FIGHTING TOTAL SURVEILLANCE WITH THE LAWS OF PHYSICS 59
THE INTERNET AND POLITICS 67
THE INTERNET AND ECONOMICS 87
CENSORSHIP 113
PRIVACY FOR THE WEAK, TRANSPARENCY FOR THE POWERFUL 141
RATS IN THE OPERA HOUSE 149
ENDNOTES 162
JULIAN ASSANGE ET AL.

JEREMIE: We also have this example of Eagle, the system sold by the French company Amesys that was sold to Gaddafi’s Libya, and on the commercial document it was written, “Nationwide interception mechanism.” It’s a big box that you put somewhere and you just listen to all your people’s communications.⁴⁵

JULIAN: Ten years ago this was seen to be a fantasy, this was seen to be something only paranoid people believed in, but the costs of mass interception have now decreased to the point where even a country like Libya with relatively few resources was doing it with French technology. In fact most countries are already there in terms of the actual interception. It’s the efficiency of understanding and responding to what’s being intercepted and stored that’s going to be the next big leap. Now in many countries we have strategic interception of all traffic in and out of the country, but engaging in subsequent actions, like automatically blocking bank accounts, or deploying police, or marginalizing particular groups, or emancipating others, is still something we are on the cusp of. Siemens is selling a platform for intelligence agencies that does actually produce automated actions. So when target A is within a certain number of meters of target B according to their mobile intercept records, and target A receives an email mentioning something—a keyword—then an action is triggered. It’s on the way.

FIGHTING TOTAL SURVEILLANCE WITH THE LAWS OF MAN

JEREMIE: So now it’s a fact that technology enables total surveillance of every communication. Then there is the other side of that coin, which is what we do with it. We could admit that for what you call tactical surveillance there are some legitimate uses—investigators investigating bad guys and networks of bad guys and so on may need, under the supervision of the judicial authority, to be able to use such tools—but the question is where to draw the line for this judicial supervision, where to draw the line for the control that the citizens can have over the use of those technologies. This is a policy issue. When we get to those policy issues you have politicians that are asked to just sign something and don’t understand the underlying technology, and I think that we as citizens have a role, not only to explain how the technology functions at large, including to politicians, but also to wade in to the political debates that surround the use of those technologies. I know that in Germany there was a massive movement against generalized data retention that led to the overturn of the Data Retention law in front of the constitutional court.⁴⁶ There is a debate going on in the EU about revising the Data Retention Directive.⁴⁷
ANDY: You are describing the theory of the democratic state which, of course, does need to filter out some bad guys here and there and listen to their phone calls on the basis of a court decision with overview to make sure it is done in the proper way. The trouble with that is that the authorities need to act in compliance with the law. If they don't do that then what are they good for? Especially with this strategic approach, democratic states within Europe are massively buying machines that allow them to act exactly outside the law in regard to interception because they don't need a court decision, they can just switch it on and do it, and this technology can't be controlled.

JULIAN: But are there two approaches to dealing with mass state surveillance: the laws of physics; and the laws of man? One is to use the laws of physics by actually building devices that prevent interception. The other is to enact democratic controls through the law to make sure people must have warrants and so on and to try to gain some regulatory accountability. But strategic interception cannot be a part of that, cannot be meaningfully constrained by regulation. Strategic interception is about intercepting everyone regardless of whether they are innocent or guilty. We must remember that it is the core of the Establishment carrying such surveillance. There will always be a lack of political will to expose state spying. And the technology is inherently so complex, and its use in practice so secret that there cannot be meaningful democratic oversight.

ANDY: Or you spy on your own parliament.

JULIAN: But those are excuses—the mafia and foreign intelligence—they are excuses that people will accept to erect such a system.


JULIAN: Once you have erected this surveillance, given that it is complex, given that it is designed to operate in secret, isn't it true that it cannot be regulated with policy? I think that except for very small nations like Iceland, unless there are revolutionary conditions it is simply not possible to control mass interception with legislation and policy. It is just not going to happen. It is too cheap and too easy to get around political accountability and to actually perform interception. The Swedes got through an interception bill in 2008, known as the FRA-lagen, which meant the Swedish signals intelligence agency the FRA could legally intercept all communication travelling through the country in bulk, and ship it off to the United States, with some caveats. Now how can you enforce those caveats once you've set up the interception system and the organization doing it is a secret spy agency? It's impossible. And in fact cases have come out showing that the FRA had on a variety of occasions broken the law previously. Many countries simply do it off-law with no legislative cover at all. So we're sort of lucky if, like in the Swedish example, they decided that for their own protection from prosecution they want to go legal by changing the law. And that's the case for most countries—there is bulk interception occurring, and when there is a legislative proposal it is to protect the ass of those who are doing it.
This technology is very complex; for example in the debate in Australia and the UK about proposed legislation to intercept all metadata, most people do not understand the value of metadata or even the word itself. Intercepting all metadata means you have to build a system that physically intercepts all data and then throws everything but the metadata away. But such a system cannot be trusted. There's no way to determine whether it is in fact intercepting and storing all data without having highly skilled engineers with authorization to go in and check out precisely what is going on, and there's no political will to grant access. The problem is getting worse because complexity and secrecy are a toxic mix. Hidden by complexity. Hidden by secrecy. Unaccountability is built-in. It is a feature. It is dangerous by design.

JULIAN: This is the bulk interception kits that can intercept half a country or a city.

JEREMIE: I'm not saying that the policy approach can work. I'm saying that this is the theory of how a democratic system would function, and indeed, even within this theory you have the secret services that are allowed to go beyond what is the rule for standard police forces and investigators. So even if we frame the behavior of the standard investigators properly, there would be other people who would be able to use those technologies. But there is a real question of whether or not we should regulate the fact of just buying and owning those technologies as opposed to regulating the use of them.

JULIAN: Like a nuclear weapon: you cannot sell a nuclear weapon easily, and some countries may want to build one but have problems. When we talk about weapons systems it's the technology that is regulated and not the use that is made of it. I think the debate might be about whether or not these technologies should be considered as war.

JACOB: It depends. When it is weapons—and there is no question that surveillance equipment is a weapon in places like Syria or Libya—they specifically use it to target people politically. The French company, Amesys, targeted people in the United Kingdom using French equipment that would be illegal to run in France, and they sold it knowingly.

JULIAN: Like selling it a whole army of trucks.

JACOB: Well, Amesys were caught with their own internal documents in The Spy Files. If we're going to talk about it in terms of weapons, we have to remember it is not like selling a country a truck. It's like selling a country a truck, a mechanic and a team that goes in the truck that selectively targets people and then shoots them.

JULIAN: It's like selling it a whole army of trucks.

ANDY: It's interesting that cryptography is regulated. There's the Wassenaar Arrangement, which applies internationally, meaning you cannot export encryption technology, which helps to protect against surveillance technology, to those countries declared evil or, for whatever reason, problematic. But if you are dealing surveillance
equipment you can sell that internationally. There are no export restrictions on that. The reason, I would say, is simply because even the democratically-run governments have a self-interest, which is to control. And even if you're dealing with evil countries and you bring them surveillance equipment to do evil things you will benefit, because you will learn what they are listening to, what are they afraid of, who are the most important people in the country opposing the government, organizing political events and so on. So you will be able to predict future happenings, to sponsor actions and so on. Here we are in the very dirty game of what is happening between countries, and that's the reality of why surveillance systems are not regulated.

JULIAN: I want to explore this analogy of mass surveillance being a weapon of mass destruction. It was a fact of physics that it was possible to make an atomic bomb, and when an atomic bomb was made then geo-politics changed, and life for many people changed—in different ways, some positive perhaps, and others on the brink of total apocalypse. A regulatory movement applied controls and so far these facilities which are now operating in full service again. So while I do agree that it would be a good idea to control this technology, I am a bit skeptical about the interests of citizens against the interests of people in power. I wouldn't even call it governments necessarily, because whoever has the ability to listen to all the phone calls has the ability to do things. This is about stock rates also—economically, you can benefit a lot if you know what's going on.

JULIAN: Where countries have legislation as to what the targets of their major electronic spy agencies are supposed to be—agencies like the NSA in the United States, GCHQ (Government Communications Headquarters) in the United Kingdom, the DSD (Defense Signals Directorate) in Australia—they have changed that legislation to include economic intelligence. For example, say Australia and the US are vying for a wheat deal, they snoop on all the people who are involved in the deal. This has been around for a long time now, at least ten years in public—but it is granted because people are doing it anyway. It started with arms deals, where you have companies like
Lockheed Martin, Raytheon, and Northrop doing arms deals, and also being involved in building mass interception systems because these groups are close at a patronage level. They got favors from their friends and covered arms deal intercepts under national security criteria. But now it applies to anything that could economically benefit a country, which is almost everything.

JACOB: A good analogy that some people in the Chaos Communication Congress brought up in December 2011 was the concept of treating surveillance technology, especially tactical surveillance technology but also strategic surveillance technology, like landmines. I think that’s a very powerful thing. Just because it’s possible doesn’t mean that it’s inevitable that we will go down this path, and it doesn’t mean that we have to get all the way to the point of every person being monitored.

There are some economic incentives that are against us though. For example, someone explained to me that the way that the Norwegian telephone system used to work is such that it would essentially run a meter which, depending on how far away your call, would run faster or slower. But it was not legal for the Norwegian telephone company to store or to keep a ledger of the actual metadata about the call you made, such as the number you dialed, specifically because of privacy concerns surrounding the Second World War. So it is possible to build that same technology in a way that is privacy-friendly but still allows for a market-based approach, which still allows for economic contributions. However we cannot win, for example, with GSM (mobile) technologies. At the moment the way that these systems are set up, not just in terms of billing but in terms