ethical responsibilities of IT professionals

andreas matthias, lingnan university
matthias@ln.edu.hk

may 20, 2010

sinclair
ZX81

commodore 64

sinclair
ZX81
SHIFT
FUNCTION NEW LINE
BREAK SPACE

ethical responsibilities

ethical responsibilities

ethical == legal?

immoral == illegal?

ethical responsibilities

morality and law

morality and law

legal but immoral

morality and law

legal but immoral

illegal but morally right

morality and law

legal but immoral

illegal but morally right

law does not address new issues

ethical responsibilities

who is responsible?

ethical **responsibilities**

to respond

ethical responsibilities

to respond
verantwortung: antworten, to answer

ethical responsibilities

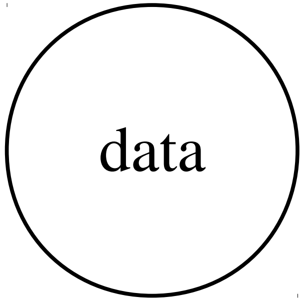
to respond
verantwortung: antworten, to answer
being “answerable”

responsible:

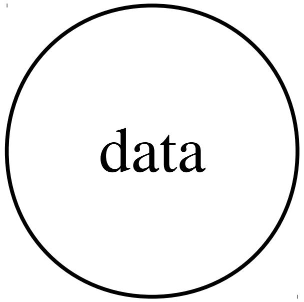
to whom?

for what?

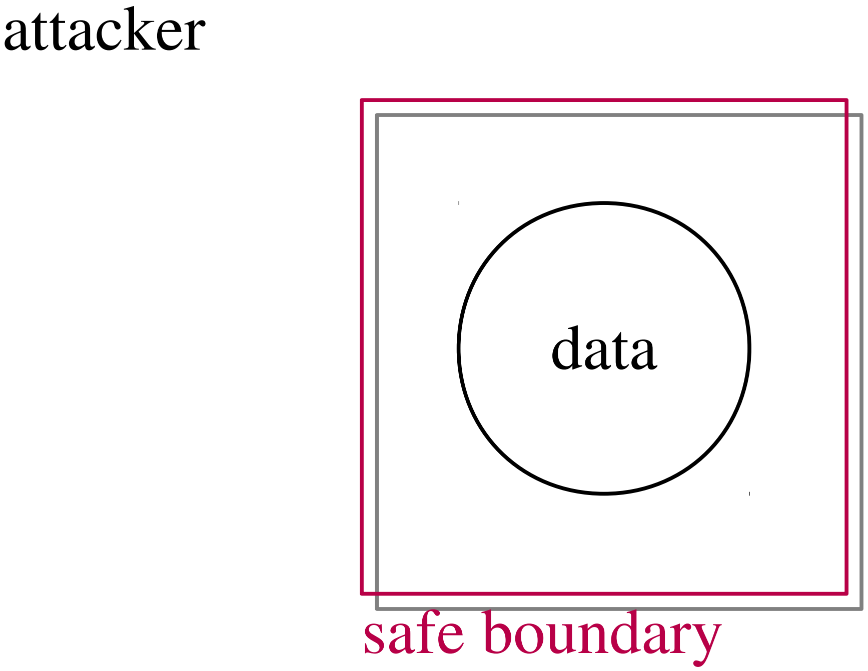
why me?

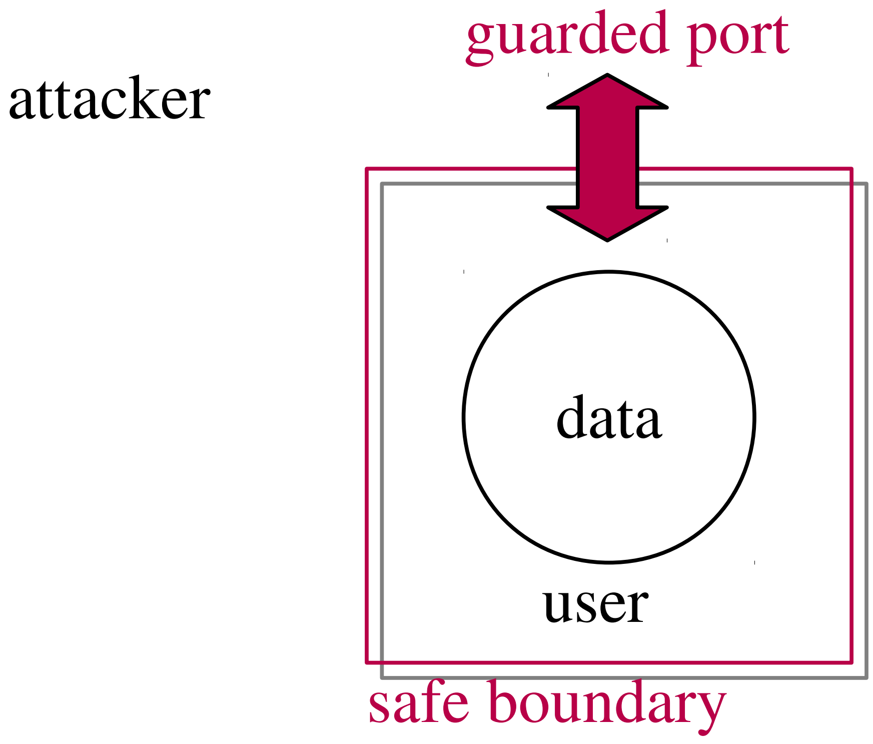

data

attacker



data


attacker
data
safe boundary



attacker

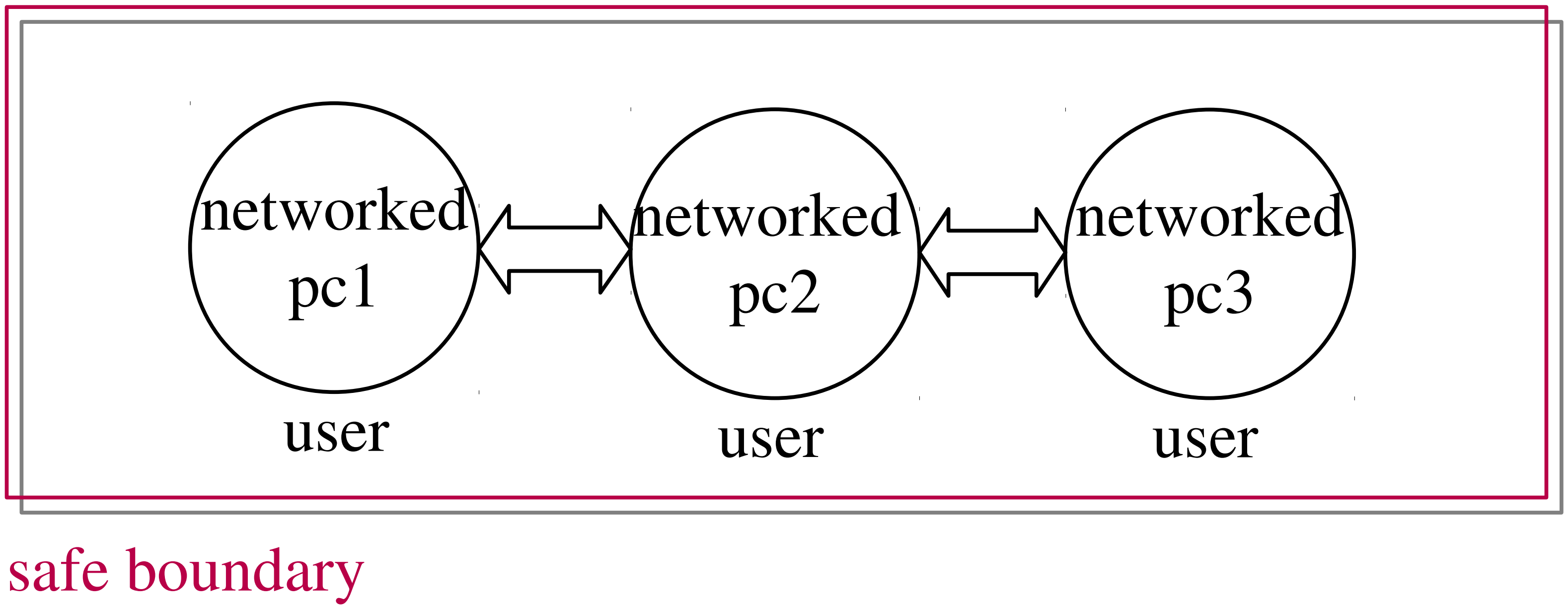
guarded port

data

user

safe boundary

attacker


networked
pc1
user
networked
pc2
user
networked
pc3
user
safe boundary

ethical responsibilities of IT professionals

responsible:

to whom?

for what?

why me?

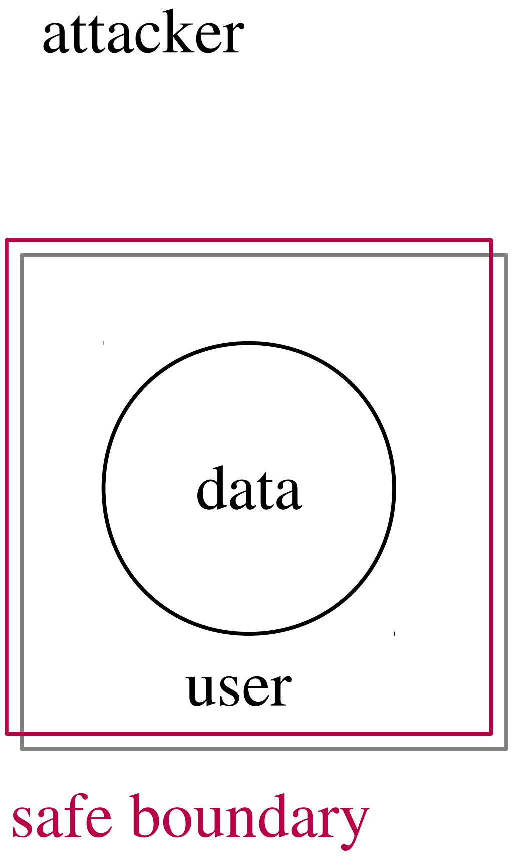
responsible:

to whom?

for what?

letters, phone calls, friendships, family contacts, access to culture and knowledge, political influence, work, free time, entertainment, love affairs, business, money

why me?

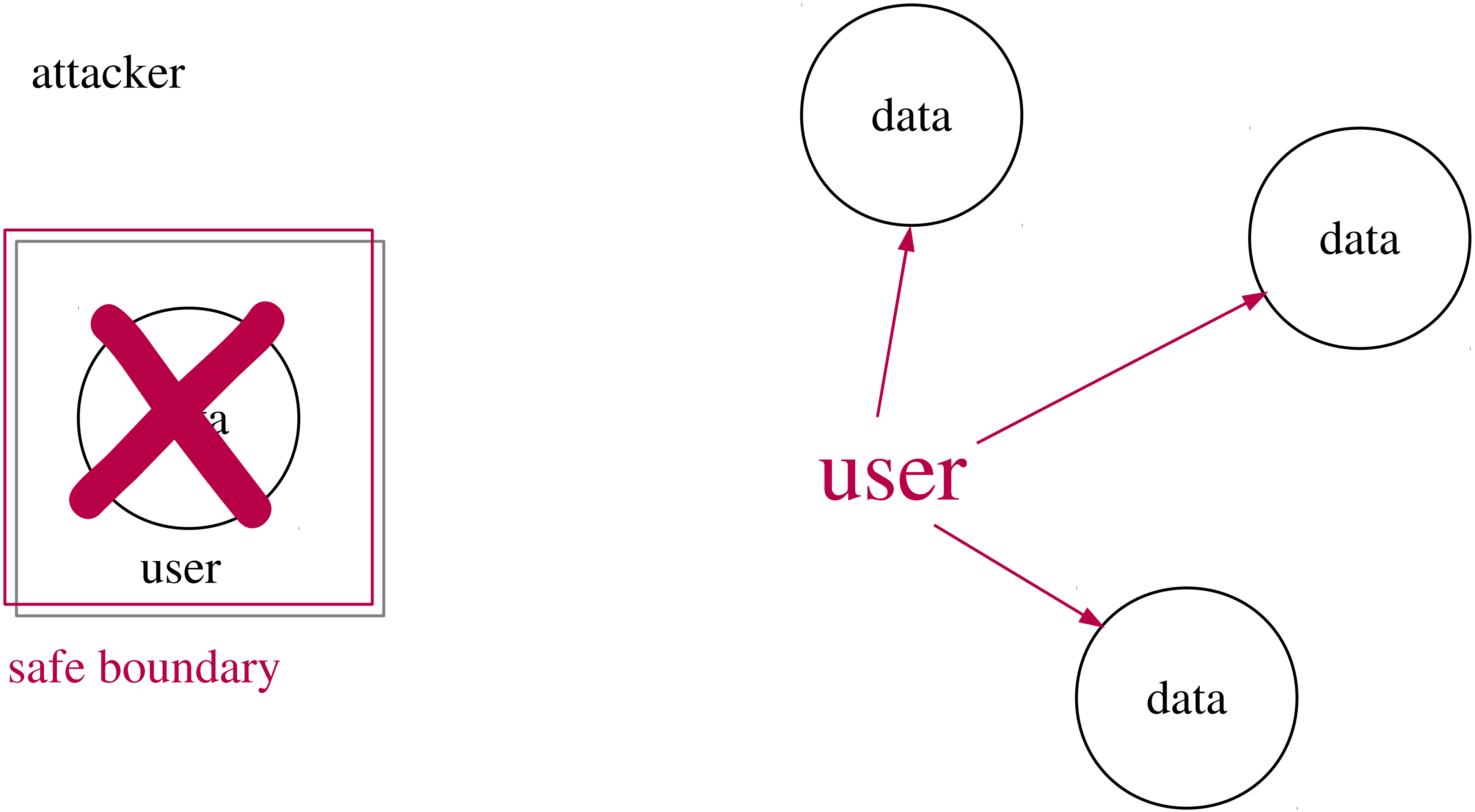


attacker

data

user

safe boundary



attacker

a

user

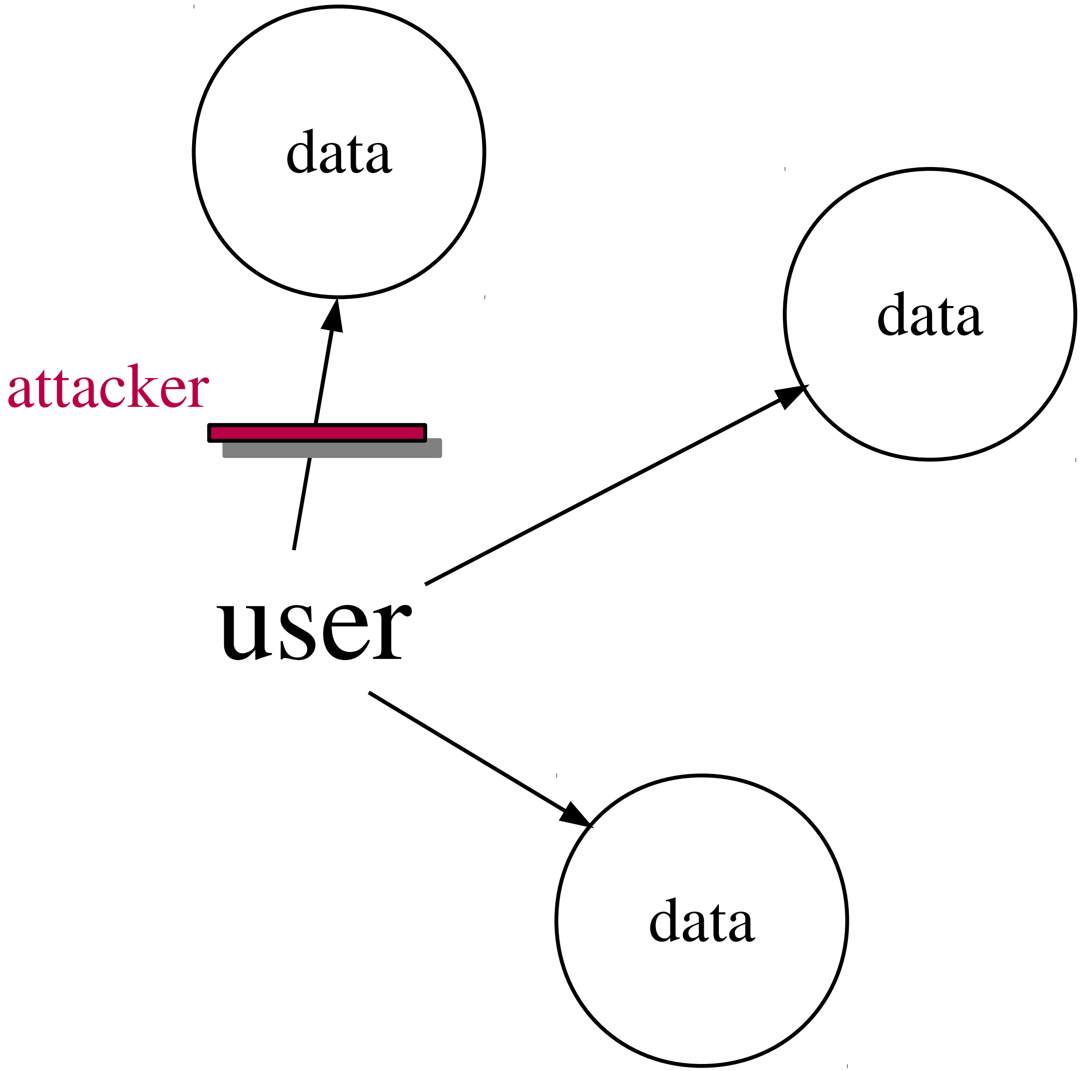
safe boundary

data

data

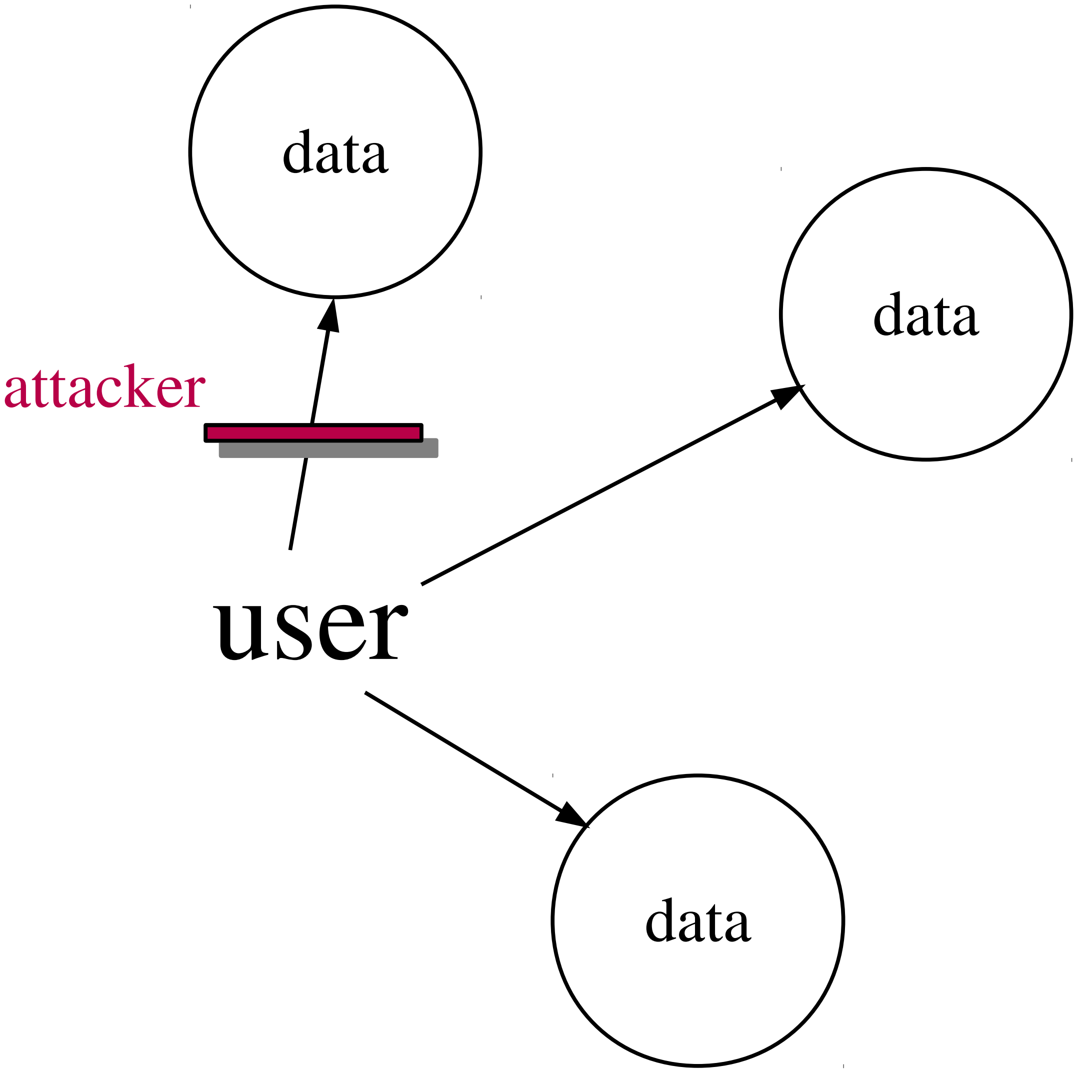
user

data


data
data
attacker
user
data

data ⇒ lives

privacy ⇒ free and safe **access**


data
data
attacker
user
data

responsible:

to **whom?** our users

for **what?** letters, phone calls, friendships, family contacts, access to culture and knowledge, political influence, work, free time, entertainment, love affairs, business, money

why **me?**

responsible:

to **whom?** our users

for **what?** letters, phone calls, friendships, family contacts, access to culture and knowledge, political influence, work, free time, entertainment, love affairs, business, money

why **me?**

responsible:

to **whom?** our users

for **what?** letters, phone calls, friendships, family contacts, access to culture and knowledge, political influence, work, free time, entertainment, love affairs, business, money

why **me?** because only you have the power to do something about it

ethical responsibilities of IT professionals

thank you!

Ethical responsibilities of IT professionals

JUCC talk, Polytechnic University, Hong Kong, 20.5.2010
Andreas Matthias, Lingnan University

Good morning, and welcome. Thank you for inviting me today. My name is Andreas Matthias. If you have looked at my CV, you will have seen that I was not always a philosophy teacher. A long time before that I had been a programmer, a webmaster, and later head of web services and of a German university's certification authority. The first computer in my life was this machine [slide: ZX81]. Perhaps some of you remember it. It had one kilobyte of main memory, and in this you could fit 26 lines of BASIC, if I remember well.

If we take one generation of people to be roughly 30 years, then most of us here today are of the same generation. My generation. And most of us will have grown up together with this technology you will be discussing today. We saw it grow out of Texas Instruments RPN calculators and home computers like these [slide: ZX81, C64]. The first real computer I ever programmed was a DEC PDP-eleven [slide: PDP11], and I'm sure the same will be true for many of you. We can measure our teenage years in the progression from tape recorders as mass storage, to floppy disks, to hard disks of ten or twenty megabytes capacity, to USB sticks, to terabyte RAID arrays.

Now the topic of today's talk is "Ethical Responsibility of IT Professionals". Reading the words, even before one has time to think, sets off several bells: one thinks of evil hackers. Of viruses. Of data protection. Of privacy. The dark guys trying to get to our servers. Spam mail. Denial of service attacks. Or, on a more positive note: Firewalls. Documentation. Clean interfaces. User friendliness. Privacy. Proper use of confidential information. Protection of intellectual property... And all the other topics you are about to discuss here later today.

I will not talk today about what you can look up in every introductory book about IT ethics. That you have to respect the rights of your users. That you have to consider the common good when making decisions. That you have to take into account the consequences of your acts. These are all important aspects of the problem, but actually forty minutes is too short a time to really go into the details of it all. And perhaps you know most of those things already. What I find interesting is a much simpler question. Look at this title again [slide: "Ethical Responsibility"]. What do the words really mean? Let us ask this question and look where it will lead us.

Lets start with "ethical" [slide: Ethical]. What does the word mean? We all know what ethics is. But is it the same as the law? Is ethical [slide: ethical/legal] the same as legal? Is unethical, immoral [slide] the same as illegal?

It would be easy and convenient for us if it were so. Because then the ethical and the legal would be the same, and we could delegate ethics over to the courts and the police. Sometimes it IS like that. When we talk about child pornography, for example. This is something both immoral and illegal. There is no justification for it on any grounds, and so it does not generate any real moral conflict. Child pornography, killing of children in schools, tax evasion of the wealthy: these are the easy cases, because we all know how to judge them, how to distinguish right from wrong and how to see the wrongness in them. Ethics begins where this boundary between right and wrong becomes blurred: a beggar, hungry, steals a cheap bun from seven-eleven. It is illegal, yes. But it is immoral? If that beggar was to starve without the bun, would we withhold it from him, placing the value of a human life lower than the 5 dollars or whatever the bun costs? You see, this is the morally interesting landscape, when law and morals part company. Only when the state and the government are not there to hold our hand and to tell us what to do: only then are we grown up and called to make our own choices, to find out for ourselves what's right and what's wrong.

There's more to this than just those contrived examples of beggars stealing buns. Let's say you want to protect your friends from harm, and so you run a password-cracker in order to see whether their passwords are good. You have no intention to use any of those passwords, you don't even look at them. You just want to alert your friends if their passwords turn out to be weak. This is clearly illegal in many countries, but is it immoral?

On the other hand, you might be monitoring web proxy logfiles in your corporate network in order to find out what the employees are doing during work time. This is legal in many countries, but is it morally correct to watch your colleagues' access to cancer treatment websites without him knowing that you do?

Things become more difficult still when you think of state laws which are clearly immoral. Most states have some of those. To take an example from the dead, which is sure not to offend anyone: in Nazi Germany, before and during the Second World War, it was illegal for non-Jewish doctors to treat Jewish patients. Jewish patients had to go to Jewish doctors. At the same time, there was a law prohibiting Jews from entering universities to study medicine. Well, you see the problem. If you were a Jew, and sick, how were you supposed to find a doctor if all non-Jews were not allowed to treat you, and no Jew was allowed to become a doctor? Of course, the whole thing was just another way of saying that Jews should receive no medical treatment and be left to die unattended. But if the state had openly said so, there would have been an outcry and protests from all civilized nations against this policy. The way they put it was clever, in that it took responsibility for the medical treatment of Jews off the shoulders of any particular person. Everyone could point to someone else. You asked your doctor, why he didn't treat you and he could say: "Well, I would, you know, but it's forbidden. Why don't you go to a Jewish doctor instead?" -- You went searching for one, but there weren't any. So you went back to your doctor and told him. "Now," he would say, "I'm just a doctor, doing my job. What do I know of university admission rules? I'm not a university administrator. You should talk to them." And, meanwhile, you died of whatever illness had befallen you.

You see how it works? There is always someone else to point to. You are safe, and you are never responsible for what happens. [slide: responsibility]

Of course, these things didn't only happen to the Nazis. Last week I was trying to pay for a particularly cheap flight to Europe I had found on the Internet, using my HSBC VISA card. Now HSBC, being security-conscious, require merchant sites to link back to an authentication module working away at HSBC's servers. Somewhere in between, there was a time-out, and I could not pay for my ticket. I called the airline's hotline. "What do WE have to do with your VISA card," they said. "It's a banking problem. Call your bank." I called HSBC, and listened for two hours to the phone jingle. As the sun was coming up, someone picked up the phone. "It's the merchant's website," he said. "In those cases, when something times out, it's always the merchant's website." So there I was, stuck in the middle of the night without a way to access my own money, and in danger of missing that ticket. I would be able, eventually, to get another, more expensive ticket. But who would pay me back the difference? Who was responsible?

Again, the system is designed in such a way, as to make no-one feel responsible for anything. The airline can blame the bank, and the bank blames the airline. In both cases, the poor girls on the phone don't have a clue anyway of what is going wrong. The programmer who really should be held responsible most likely worked for a contractor and was now on some other job entirely, perhaps sipping a cocktail somewhere on

Hainan Island, being able to pay with his VISA card of some other bank which had properly debugged their system.

So now we've talked a bit about two of those words already. Ethics, which is not the same as the law. Laws can be immoral. [slide: three possibilities for law vs. morality] Acts, which are legal, can be immoral. Acts, which are illegal, can be morally right. Or the law might just not address some issues, which is a common case in high-tech, and then the only thing you've left to judge right from wrong is your own, private, moral intuition.

That other word is responsibility [slide: who is responsible?]. We saw that the way our society is organized tends to keep responsibility away from those who are, in fact, responsible. The system puts up layers upon layers of phone support officers, outsourced customer service, changing private contractors, and clueless employees, which make sure that no particular person ever feels responsible for all the little things which go wrong in our lives every day. For the big things, we can always bring the bosses to the courts. But if I miss that flight, who is going to take responsibility? The boss of HSBC? The airline's boss? Or the phone support girl?

So here we find the first problem: The responsibility is something everyone loves to talk about, but, in fact, the moment it counts, we do what we can to avoid it. And the whole system of our operations is designed and optimized to allow us to do just that: to escape our responsibilities. To point to the other guy, who can then point back to us, closing the circle in which our victims are trapped. This is why I think that talking about moral theories alone does not help much. Long before we talk about morality, the first and most important step is that we must get used to accepting our responsibilities and not to point to the other party over there. The system all around us makes it so easy to escape our responsibility, that we must actually practice to recognize it. We must know when it really IS our job to take care of things which go wrong. Simply because there is no one else there to do it. If we don't act when we are, in fact, responsible, then this in itself is immoral behaviour. We don't need to actually DO anything bad. Looking away can be as bad as any immoral action.

Now, if we think about responsibility [slide: responsibility] for a moment longer, we find some more interesting questions.

Responsibility, the word, comes from "respond". Responsible is someone who has to respond to me about something [slide responsibility: respond; Verantwortung: antworten] I have a question about this or that, and someone is there who has to respond, to answer me. He is "answerable" [slide] as we say. So this poses a few more questions. If I am responsible, if I have to respond, then naturally I can ask: responsible to whom? for what? and, above all, why me? [slide: responsible to whom? for what? why me?]

Let's look at those questions in turn. You remember, we talked in the beginning about generations, and about what computing used to be. For many of us, some of these memories are still there, and they still influence the way we see the world of IT. And this can lead us to wrong assumptions about our role and our responsibilities, because the world has changed.

In old times, we used to think of our computers and security in a metaphor of inside versus outside. This is my home computer [slide] and my data is inside it. The bad guys are outside [slide]. Now this is the same situation I have with my house or my apartment. The valuables are inside, the burglars are outside. Or, to speak morally, the good are inside, the bad are outside. Between the two regions there's a boundary: an apartment door, the walls, a lock [slide]. My computer also has doors: USB ports, or disk drives, from which bad things (viruses, malicious code) can enter the inside, which I want to protect. I have network services listening on ports, [slide] which are just like more little doors, from which the bad guys can enter. So I build more walls, fire-walls, I lock down the unused ports, I block access to them by filling in the doorframe with bricks, leaving only those doors open I really can't do without: one port for the service the machine performs, and perhaps some secure shell access. The same, of course, applies to whole networks [slide]. Again, there is inside, the trusted area, and outside, the realm of danger.

This, in short, is the essence of the old computing model we all grew up with. The computer system as a protected space with precious data inside and dangers outside, and the war is going on at the boundary between in and out, regardless of whether we are talking about single machines or networks.

It is important to see that this model, although it does not represent a significant part of reality any more, is still at the heart of much of what we believe to be computer security and computer ethics today. You know the old saying: the only safe computer is one which is locked up in a closed room, behind a steel door, and not connected to anything else. This is the model of inside/outside security.

If I take this seriously, then what can I say about the ethical responsibility of IT professionals? The good stuff is inside, the bad world is outside. Whom am I responsible to? To whom do I have to answer? Obviously, to those who are inside, those whom I, the administrator of the system, have to protect from the outside world. If I have only a personal computer, then the only user who has any assets in my system, is me, myself. I am answerable to myself alone. If I mismanage my system's security, it is me who will suffer, my data will be lost. Now if I open a second account on my system and I have one user, and this user uploads data to my system, then I am also answerable to him. This classical model scales up to the size of companies and universities without much change, and it is at the heart of Unix system administration. The user called "root" is responsible to his users for the safety of their data.

Now the problem is that this model is not the reality any more. Over the years, one little step after the other, the situation has changed, but we may not have taken enough notice of that change. Many of us are still doing IT security and IT ethics as if we were on a mid-1980's Unix system. We just got used to think of the *network* as our system, kind of a bag full of CPUs and storage, connected by wires, but not really different from what we used to be in charge of when the users still called us "root". But things are different now.

First, there is no inside any more, and no outside. "Our" users are not "our" users any more. Sometimes we host their emails. Sometimes a little storage space. Sometimes we just administer their local storage in a Windows network. Sometimes we don't even do that, and all our data is just a login identification record. We surely don't host the users' most precious data any more: their documents are on Google docs, their friends are on Facebook, their pictures are on Flickr, their movies on YouTube. University file service is next to dead, and with it goes all the simplicity of the inside/outside security model. Instead of the apartment, where we used to guard the door and change the locks, now we're left with an empty bag, on which is printed the user's name and some metadata, just enough to let the users open a browser on a public Internet workstation. So what are we still responsible for? What do we have to answer to our users for?

The other change is even more profound. We used to think in terms of data. IT security as data security. What was at stake if data got lost, was the value of those data. Essentially, again, we were guarding a closed bag with some valuable things inside. This is no longer the case. In the old times, our users had a job, they had friends, they wrote letters, they read newspapers, they watched TV or read books and magazines, and somewhere among all this they also had a few files with data from their work. If the files were lost, well, then they were lost and the user had to find the data again or re-write his documents. This could be a nuisance, but it was almost always a limited damage. IT failures were, with few exceptions, not life threatening.

Of course, we all know that this is not the situation any more. Our users today, whether they know it or not, do voice over IP. There's no telephone any more in the sense of Alexander Graham Bell. There still is a post office, but who uses it? We write letters through email, we keep in touch using instant messaging tools. For two years now, I meet my friends more often in Facebook than outside of it. My family back in Greece I see only on Skype, once every week. With the exception of my wife and my classes, I don't have any purely off-line social life any more. My money I can access only through computers. If the computers don't work, I can't buy a flight ticket, and I have to stay at home. If the computers don't work correctly, I indeed don't possess any money. Whatever I own, is nothing but a database record somewhere on an HSBC server. My books I order through Amazon. My political facts and opinions I get from the BBC website. A big part of my entertainment from YouTube.

You see, this is the second problem [slide: Ethical responsibilities of IT professionals]. It says IT, and we pretend that we are still talking of IT here. Information technology. Files and directories. Not true. "IT" is no longer information technology [slide: Responsibility: for WHAT?] What we are answerable for, if we like it or not, is not a handful of files. What we are answerable, responsible for, is life itself. The lives lived by our users, their letters, phone calls, friendships, family contacts, their access to culture and knowledge, their political opinions, their networks of work and private responsibilities, their free time, their entertainment, their love affairs, their business, their money. All of this is nowadays "I.T." And all of this has been put by the development of technology, into OUR hands to take care of and to safeguard.

This then, is the reality of it, which we perhaps would prefer not to see by looking away. [slide: Responsibility: To whom? For what?] Our responsibility is not only to keep hackers out or to remove viruses from hard disks any more. While we were busy doing this, the users uploaded their lives onto our systems, and there they are now, lying open and unprotected, and waiting for us to make sense of how to safeguard them. Lives, not data. People, not information. We have tremendous power over human lives, over social processes, over structures of power. Think about it. No government can reign without us, no crime to speak of can happen without our collaboration or mistake, no Nobel prizes can be given, no education funding can be planned, no hostel rooms allocated, no friendships made, no flight tickets paid, without one of us being always somewhere right in between those processes, coordinating them, taking care of them, making sure they work, or making sure they don't. So then, if we are those who are equally necessary to collaborate in and to support both the good and the bad acts, both the crimes and their investigation, then this is why we have this enormous responsibility. Our moral standards, our behaviour, will not only affect a few files on some server. But it will profoundly change the lives of hundreds, thousands of people, will promote their careers or threaten them, will help them live as free, happy, informed, powerful citizens, or condemn them to lives of isolation, frustration, illiteracy, and slavery. I am not exaggerating. My own career depends on being able to read philosophy journals. This one little entry of a few bytes in my university's Radius server makes all the difference for me between a life as an active, publishing researcher and a life outside of academia, cut-off from the only resource I need in order to be able to work. Delete those twenty bytes from the user database, and I'm done for, unable to earn my living, unable to do the only job I was trained to do. Delete my Facebook account and I lose my friends and my social network. Delete my IMAP account and I can't communicate any more. Delete twenty bytes in my bank's database and I'll have to go live under a bridge, because my money will be gone.

Therefore, it seems that the traditional model [slide] of us protecting the valuables INSIDE a closed, protected space, is wrong. The valuables now, the users' data, are all somewhere OUT THERE, hosted by Google and Flickr and Facebook. Our job is not any more to keep the bad guys out, but [slide: the new model] since now the user is separated from his outside data, to secure ACCESS of our user to the services and data which constitute his or her online life. The role of the bad guys, conversely, is not any more trying to break in into secure spaces (at least not as long as we are concerned, since the secure, closed spaces are now managed by Google and Facebook and are not our problem any more). The enemy of this new model [slide] which is centered on access to information, would be everyone who tries to block that access.

This is a radical redefinition of what we are supposed to be doing in computer security, and it fundamentally affects the question of our ethical responsibilities as IT professionals.

1. [slide 1. data->lives] First, we are no more concerned with information and data; we nowadays handle lives and online social structures.

2. [slide 2. privacy->free access] And secondly, our and our users' main issue is not any more data privacy. Privacy CAN be important in some areas like Human Resources or medical insurance claims processing. But it is not the main concern of the majority of users. Our users, both scientists and students, write their papers on Google docs, without any concern about who might have access to them behind the scenes. They post their CVs on their webpages. They publish their preferences on everything under the sun on Facebook, along with a day-to-day logfile of their activities. Their travel images, the names and faces of all their families and friends are publicly available, just a mouse click away. Privacy concerns, as sacrilegious as this may still sound, are more an academic interest of a few data ordinance officers than they are a concern of our users. What really concerns the users, though, is access to data, theirs and their friends'. Access to email. Access to Facebook. Access to Google. And this means, FREE access, both in the senses of freedom from costs and freedom from censorship and control. The users' hunger for free access includes areas, in which such access might be illegal: access to music files, for example, or access to commercial movies. But they go to great lengths anyway to secure that access, installing peer-to-peer networks, setting up their own servers, or trading DVDs with their friends on campus. These activities are illegal, sure, but to what extent are they immoral? This is an ongoing and as yet undecided debate in computer ethics, and each one of us will have to make up his or her own mind as to how to deal with copyright infringement for personal entertainment purposes.

We were talking about access, and I just used this as an example of really how much access is worth to today's users. In a sense, we see a reversal of the traditional model here: originally, the user's interest was in protecting his or her data from unauthorized access. This has been changed by the data migrating into public spaces, where privacy is a secondary concern (if at all), and FREE ACCESS becoming the premium commodity, which the adversaries of the free Internet are trying to block. In some ways, this mirrors the process of the historical evolution of societies. Access to commodities has always been one of the main driving forces for social progress and the primary goal of modern, democratic societies. And much of human history is the history of trying to gain access to something valuable. Access of the workers to the means of production. Access of the underprivileged classes to knowledge. Access of the black population to the front seats in the bus. Access of the people of India to the sources of salt. Access of the working classes to social status. Access of all citizens to the functions of political power. And now, as the world becomes digital, access of all citizens to the sources of knowledge, of entertainment and to the social structures and the means of exercising political power which are available in cyberspace.

It is obvious now, that the old *Feindbild*, the picture of the enemy being an undernourished and badly groomed Russian teen-aged hacker, is not adequate any more. Hackers and viruses surely exist, and surely they are a nuisance, and surely they must be fought. But not at the cost of overlooking who the real enemies of the new, open society of the Internet are: namely those, who have an interest in severing the free access to information [slide]. The classical teen-aged hacker type has no interest to do so.

It is quite obvious WHO has an interest in blocking access to information. There are various motives. Financial profit is one of them. I don't say it is immoral per se, but it endangers free access of people to their online lives and must therefore be watched with suspicion. Protection of the interests of the media industry is legitimate, but no free society can allow financial considerations to be put above the welfare of its citizens, above free access for all to cultural artifacts and sources of knowledge. So here is one potential enemy of the open information society: the media industry. Despite its trying to restrict access to a great part of mankind's recent cultural production, we, as the citizens and the guardians of the online world, must recognize that its interests are only part of the total society's interests and they must be weighed against other interests regularly and with care. If today's copyright laws had already been in force six-hundred years ago, there would probably never had been the literacy revolution which started with Gutenberg and his printing press. Literacy, and learning, and science, all require a reasonably free flow of information and free access to resources of learning and knowledge. If this access is restricted, you get the sterile intellectual environment of the medieval monastic scriptorium, a place dedicated to copying the same restricted materials over and over again. Whether our information society will stay open to learning and innovation or whether it will degenerate into a stifling dictatorship of controlled access to knowledge and art, is something which we, all of us, must not allow the media industry alone to decide. We ARE the state, all of us, and they are only a tiny part of it.

Another danger comes from governments, especially the demand for a traceable personal identity of internet users. With the fashionable pretense of fighting terrorism and crime, governments world-wide have severely restricted civil liberties, privacy and freedom. This, of course, applies to countries east and west alike. What we citizens are supposed to overlook, is the fact that many, if not most, of these measures, which are said to fight terrorism, are actually only of use in effectively controlling and restricting the civil liberties of the majority of citizens, without in any way deterring terrorists. Take an example: In Germany, you have to register your cell phone with your name and ID card. You can't buy a phone anonymously. Does this really help fight terrorism in any meaningful way? Are professional criminals really so clueless that they can't steal a mobile phone from a shop or from the pocket of a tourist? Criminals who have access to guns and bombs are supposed to be unable to get hold of a mobile phone?

Or, take an example from Hong Kong: the personalized Octopus card sounds like a great idea, until you realize that with it you are giving away a complete logfile or all your movements and all your purchases. With it, the government and companies who participate in this scheme know more about your life than you do yourself. Do you remember where you have been on the 16th of last January? Well, they do. Again, it is control as opposed to freedom. Restricting open, uncontrolled access in the interests of profit, or better monitoring, or targeted advertisements. This, again, has no positive effect on security. A criminal who handles machine guns and drugs for his daily income will not have problems finding a stolen Octopus card or paying his bus fare in cash. Or, take China, where to access the Net you have to identify yourself first with your ID at the Internet cafe's staff, so that your forum postings can be traced back in case you write something you shouldn't. Is this deterring criminals? Can't criminals fake ID cards well enough to fool an Internet cafe employee? Again, the point here is not to control the criminals, but to take away free speech from the citizens who are entitled to it.

What is fundamentally wrong with this approach, is that it is based on two fictional assumptions. First, that all actions, which are against the interests of a government, constitute criminal terrorism. This, of course, although it is an assumption shared by many major governments today, is a danger to a free society, which must acknowledge and protect minority rights and free speech for all, and in particular for those who oppose the government. Rosa Luxemburg said, "freedom is always the freedom of dissenters," and we should be careful to protect the dissenters, because we might be among them one day. Second, even assuming that we talk about legitimate, real crime, it assumes that repression of freedoms and police action is the only appropriate response to it. Spelled out like this, we can immediately see that this assumption is not true. It is not true, because it neglects the reasons for crime, and the known fact that it is both easier and more efficient to combat crime by improving living and education standards in a society instead of putting people into prisons. In Germany, recent statistics show that about 80% of prisoners will go to prison again at some time after their release. Police action does not constitute a real solution to society's problems.

Let us stop here and return to the original question [slide: Responsibility of IT professionals: For what? To whom? Why me?]. We've answered the question WHAT we are responsible for. It is the online lives of our users, the free and open society of the Internet, no less. To WHOM we are responsible is equally clear: our customers, our users, the people who entrust their online identities to us, who use our services to meet their friends, pursue their careers, access sources of knowledge, fall in love, have fun, study, and pay for airplane tickets. These are the citizens of the civil society, and to these alone are we responsible for how we promote or endanger their interests. Laws can sometimes be an indication of what is moral or immoral, but no more than this. Often laws are made by particular lobbies, and often they are dangerous and immoral, and not in the interests of the citizens. Much more so if those laws are not legitimized by democratic procedures, and thus don't express the will of the majority of society's members.

Now, if all this is part of what is meant by "Responsibility of IT professionals", then it seems that the topic is getting a bit out of hand. I'm a programmer, you say, or the head of the web services team at a university's computing centre. I have enough work to do as it is. Why on earth is it MY job to defend free society? [slide: why me?] Why, indeed.

Perhaps because we, the technicians, the programmers, the IT experts, are the only ones who CAN do something about it. Remember, for a moment, the problem of my credit card payment which didn't work that night. Who COULD have done something to solve the problem? The telephone support girls could not. I could not. The airline's hotline could not. Even the bank manager probably could not. There was only this one guy who programmed the thing without really caring to do it well. This one person was the one who really COULD have done something to solve the problem, perhaps by thinking a bit more, perhaps by being more careful, by anticipating server load and network lags. He is responsible simply for the reason that he was the only one who COULD have solved the problem. And he failed, because he didn't.

Now you are all in the position of being those who really DO things in this new online world. You are always there, organizing IT services, planing access solutions, overseeing programmers, tweaking Radius servers, storing or deleting logfiles, running databases well or badly, keeping users' data safe and their access free and secure. Or giving them away to those who have an interest to threaten the system, to abolish freedom, and to convert the lives of free men into shopping malls and prisons. You are not Google or Facebook. But you are still responsible, simply because you are THERE, at the access point, at the interface between the user and his online life, at exactly the point where this connection is always at danger to be cut and be replaced by something more restrictive, more controlling, and perhaps more immoral. You didn't ask for this power, but it has been given to you, and now you have to deal with it. Without your help, many bad things can't happen. Without your collaboration, no one could access your login server's logfiles. Without your help, no government could spy on Internet forum use. Without your help, no emails and no Google searches could be censored. You have the actual power to do the right and the bad thing dozens of times every day, every time you agree to set up a log file, which you know will be misused, but also every time you pretend that your software does not support logging or that a file was accidentally deleted, or that a hard disk crashed and the data is gone. Your fingers are, literally, at the buttons of power. The buttons which control not only the freedom all of us have today, but also the freedoms our kids will have in the future. It all depends on you. You are the IT professionals, and you ARE responsible. For our lives and for the freedom of our society.

Thank you.