Commissioner Bob Paulson presents keynote address at the Securetech 2015 conference

November 25, 2015
Ottawa, Ontario

Speech

Check against delivery

ORIGINAL SOURCE: http://www.rcmp-grc.gc.ca/en/news/2015/27/commissioner-bob-paulson-presents-keynote-address-securetech-2015-conference

Ladies and gentlemen,

Thank you for the invitation to come and speak to you today.

My intention is to speak today about, loosely framed, policing the Internet or, some of the technological challenges we are facing as we come into this new era of technology.

I want to put this out on the floor and then maybe we can talk about it. I understand that folks want to have questions and answers later, so I am happy do that to the extent that you have the time to do that.

I am going to introduce Paulson's paradox. It's not particularly complex and some people make fun of me for having it, but it goes something like this:

Security means little to those who have it, and it means everything to those who don't. So as I begin to talk about some of the issues that I want to put before you, that's what I'd like you to keep in mind.

Because fundamentally what my message is here today, is that the trust and confidence in policing is absent in the cyber world – in the information management world.

And historically, we have had success in policing, where we have had that trust and confidence, and so that's going to be the focus of my comments.

So almost 30 years ago I started policing in Chilliwack, British Columbia, and when I did, I soon learned, because my bosses were hammering it into my head, that I had to know who I was policing, who these people were that I was asked to police.

So we're talking about cab drivers, school teachers, clergy, Aboriginal leaders, crooks, bartenders; in short, all the people that make up a community. And the reason that was, was so that they would talk to me. Not so I could talk to them, but so that I could listen to them about their policing needs and have them participate in the policing process.

So our mandate here in Canada, certainly the RCMP's, according to our Act, is to both prevent crime and apprehend offenders. And we can do neither without the cooperation and consent of the communities. Because policing fundamentally is an information-based business.

We need to know who the next crop of burglars are; we need to know which kids are being abused in the community; we need to know who is walking the streets at 3 o'clock in the morning slashing tires, holding a crowbar, holding a screwdriver, holding a knife.

We need to know which people are moving up to hard drugs and will soon be breaking into people's houses to get the money to fuel that, and eventually robbing corner stores or banks. And we need to know who's coming into bars with blood on them. We need to know who the bad trick is that's abducting, killing and harming sex-trade workers. We need to know who the youngster is in the basement that's radicalizing his mind to violence as he looks at some of the material on the Internet.

And good information is gold, it's absolutely vital to our success and it doesn't just fall into our lap. We have to have people give it to us. And without that trust and confidence that I referenced earlier, we're not able to get that.

When we look around the world, and just recently in Chicago, there seems to be a separation of police and community, and that trust is being dissolved.

You have to ask yourself why that's happening, and there are a number of very, very complex contributing factors; probably a very complex swirl of social and economic inequities, cultures, history, policy choices, police behaviour.

Fundamentally though, the cause is the outcome. The police and the community are separating because the police and the community are separating. It's an us-and-them type situation.

And in the information management world, where privacy now is driving a lot of the concerns around the state wheeling into a community's information, we're just simply not trusted. The police are not trusted to manage that information.

You know, Sir Robert Peel talked about the police being the community and the community being the police, and that's never more true than in today's modern, technologically driven society. But we haven't been able to make the switch into how that gets transferred, how those policing values, how those policing styles, how that community engagement with our policing strategies gets translated into the digital world.

There's also another end to Peel's advice, and that's the community has an end, has a responsibility in that balance between police and the community. And their end is to be informed of what the issues are, and I think our colleagues here in the media, government officials, do a good job of trying to get that. But the complexity of the issues that are facing us now on the Internet and security-related matter are very, very complex and they can't just simply be understood, you know, in the turn of a 15-minute blitz on the television, cycled through our news cycle, 24 hours a day before we're on to the next thing.

Communities have to consent to being policed. We see some examples of that in our lives. At airports for example, people know what they have to do to get onto an airplane. Line up, empty your pockets, you know, take off your shoes, take off your belt, where are you going, where are you from? People do that and they go along with it because they understand, they understand what's going on there. It's intrusive, but they get it.

But the more safe and secure we are, the less interested we are in the things that keep us safe and secure. One of the risks in living in a free society is that we forget all we needed to do to become so free. Today we'll abide nothing that can remotely be seen to be interfering with our privacy.

Freedom and privacy are being interchanged. I don't know if that's a fair way to look at the issues. The truth is, the average Canadian is probably more at risk, their privacy is probably more at risk from the things that you do in this room – from commerce, than they are from the state.

We don't have a full understanding of what that means for our citizens. Citizens are concerned about having their privacy invaded by the state, rightfully so.

But our privacy has to be thoughtfully and carefully balanced against the very communal dimension of our existence.

We can't have anonymity be a substitute for freedom. It can't be understood that anonymity is the standard by which we will go about living in a social environment.

The truth is, the world is a messy, unsafe place in many respects. The complexity of the issues and the precision around decision-making in that context cannot be fairly represented in a sound-bite.

Truth is, that if people really understood our business in the security world, they'd be very grateful for the professionalism and attentiveness that our men and women have for their freedoms, for a citizen's freedoms. But that isn't 1984, and it's kind of cool to be anti-establishment again.

Take for example this reason I am speaking to you here today. I'm proposing… You know, we've had discussions around going dark. That is a very live discussion in the policing world. And particularly in the counter-terrorism context, we talk about going dark understood as technology overrunning the police ability to access evidence to support criminal justice outcomes. That was a little more complex than it was in my head, so let me go back to that.

The Internet is a place, it's not a thing. It's a place full of really smart people doing really cool things, really quickly. But a lot of them are bad. Some of them are bad. And the ones that are bad are getting badder, and they're happening more often.

Criminals now are live-streaming child-sexual assaults that are being committed to order so as to avoid leaving the digital evidence on the web.

Billions - billions with a b, billions of dollars of criminal proceeds are being laundered through the Internet. Multi-national criminal organizations are effectively running their affairs on the Internet, and that's just a few examples.

There's bank frauds, there's identity theft, there's credit fraud, there's extortion, there's sextortion, there's drug trafficking - on and on and on the list goes.

But thinking back to Chilliwack, just as I couldn't keep those people safe and do my role as a police officer if I didn't know who they were – if they went about their business in the community of Chilliwack, day-in-day-out, with masks on, or wrapped up in sheets, or driving vehicles without license plates, or their plates were covered up, or leaving phone numbers that could never be looked up or living in houses that didn't have addresses, on streets without names – I couldn't do the job of policing in that context.

It's a very difficult proposition to bring traditional criminal justice strategies to bear in a place where anonymity is protected.

Now I will say about going dark; the encryption that is developing and providing all sorts of advantages and you know, I don't want to insult you by suggesting that there aren't commercial competitive advantages to having your communications encrypted, there are. That ought not to be the Holy Grail of policing as we enter the technological world.

So we could argue, and it's a risky proposition to argue for laws, and we've seen what happens sometimes when police take advocacy positions on laws, it doesn't always work out, and sometimes we're ridiculed as being, a), the wrong people to be doing that, and b), wrong.

But, the idea of going dark is not a new one. I was thinking of this as I came to speak to you here at noon. I used to chase bikers out on the West Coast, the Hells Angels in particular, they were very difficult to catch, because they had gone dark. And they hadn't gone dark technologically, they had gone dark in their behaviours.

They wouldn't talk on the phone, they wouldn't write criminally relevant communications to one another on their computers, they wouldn't write criminally relevant communications on paper. When they would go and talk dirty business, they would go off into a field and whisper into each other's ears. So effectively they'd gone dark on us.

The solution couldn't have been to make them use their phones. That's not going to work. We're not going to create a law that says, ok, if you are organized crime, you must use your communication devices so that the police can intercept them.

We had to change our thinking, and we had to engage key partners in communities with regulatory powers, with other powers to be able to bring the full weight of an organized society to bear on criminal conduct that was going unchecked. And in the end, we were able to bring some successful prosecutions against them. That didn't sort of eliminate them from the face of the earth, but at least put their criminality where it ought to be, which is on the crime side. Those people are crooks, everybody knows that they're crooks.

So the similar approach needs to be brought, I think, to technology. We're chasing the wrong Holy Grail. I am all for new legislation, I am all for warrantless access to subscriber info, you know, if I had to get a judge on the phone every time I wanted to run a license plate when I was doing my policing, wouldn't have been much policing getting done. That's not my call. That's not the police's call. That's our call.

And I think that is where we need to take this conversation, that we can't have people exploiting our citizens to the extent that they do, and that we will demonstrate that they do, in numbers, in dollars in children hurt.

Children… in the child exploitation world are being hurt at a pace and a frequency that is alarming. And I tell you the irony there, because technology is fueling that. So now these people can encrypt their communications and they can exploit children for sexual purposes and it's a little harder to get at them from the police point of view. And the discussion around child exploitation is a difficult one, because nobody wants to hear it.

It's like you're on a jury at a murder trial that's particularly violent. You don't want to see the pictures of that. It's offensive to the average-minded Canadian to know that that sort of criminality is going on. And the answer isn't to put it in your face all the time, and say, hey look, we've got some serious problems over here in policing. It isn't. Or maybe it is. Back to my trust and confidence in policing.

So my proposition is to chase down the laws where we can, where they are consistent with Canadian values and the Charter of Rights and Freedoms, and make sure we have a sensible framework in which we can access subscriber information, but also to engage people, you people, in the discussion around keeping our citizens safe in this new world that we're building.

The Internet is marvelous, it's as though we created this thing that has limitless potential for commerce, communication, education, access to information. It's limitless.

But we also say, okay, wait a second now, but no rules, no rules. And that's fine, that's fine, if we don't want justice there. But people are coming to us now, people are coming to the police and saying, hey, I was victimized on the Internet. Companies are coming to us saying hey, my exclusive information was stolen through the Internet. Governments are coming to us and they're saying, hey these people are infiltrating our databases and violating the privacy of individuals.

It's a serious problem, and they're coming to the police for a just outcome. Investigate this, find out who did it, and bring them before the courts. And that has all sorts of complexity attached to it. And it's not just our problem.

I am happy to be the spokesperson for the problem; I guess that's what I'm doing here today. But it's our problem. Your safety, your family's safety, your financial integrity is at risk. And so we need to start having the conversation now, and my partners, our partners in policing, in the U.K., the United States, Australia and New Zealand, we're all on the same page. We're all struggling with this.

In fact, I was just in Chicago and had occasion to speak to folks on this very topic, about what are we doing and how are we thinking about justice in the Internet. How we are thinking about reasonable limits and making sure that people are kept safe. Because fundamentally, ladies and gentlemen, it's hard to keep people safe on the Internet right now. The best advice I think we can give people is either, a), don't go, which is not working, or b), if you go, be really, really, really careful, and if something bad happens to you, you know, hopefully we'll be able to help you. But there's no guarantee.

So, people who enjoy security don't often think of security. People who don't have security are obsessed by it, and all the attendant issues between the left and right arc of that proposition are before us. So I would ask that in your deliberations, in your discussions, in your technology development, that we begin to have those discussions. Not that you need to be recruited by the police. You need to think about your community's safety.

So those are my comments, thank you very much. And if there are questions, observations or challenges, I'll see how long I went, I went as long as I ought to have went. So thank you ladies and gentlemen.

–30–

#