Edward Snowden at the MIT Media Labs Forbidden Research Conference:

Note: this transcript may not be 100% correct.

Snowden started bay saying that there wasn't enough talk about the "idea that laws are actually a weak guarantee of outcome.

"We outlawed murder, we outlawed theft, they still happen. We outlawed many other behaviors, they still happen. This is not to say they [the laws] are bad, this is not to say we don't want any rules. But there are better guarantees, and we should consider when they are appropriate. And when they in fact can provide a greater enforcement for individual human rights than the actual laws or policies themselves when left naked and sort of *[unintelligible]*.

"Some years ago I told the truth about a matter of public importance and as a result a warrant was issued for my arrest, and I am no longer able to travel freely. But today is a great example of why that doesn't mean exactly what it once did.

"And because of that I'd like to thank very much MIT for organizing this conference, and the opportunity to speak with everybody here today. For journalists in the audience, that's not a small thing. I should point out that they deserve credit for living up to that commitment to knowledge. Now, no organization is perfect, everybody makes mistakes, but that is quite a risk. And this maybe the first time, an American exile has been able to present original research at an American university. It's hard to imagine, I would say, a more apt platform for this talk than the forbidden research conference. But that's enough preamble.

"The guiding theme of many of the talks today, I think, is that law is no substitute for conscience. Our investigation regards countering what we're calling lawful abuses of digital surveillance. Lawful abuse, right, what is that, doesn't seem to make a lot of sense. Seems like it might be a contradiction in terms. (…) But if you think about it for just a moment it might seem to be a little bit more clear. **After all, the legality of a thing is quite distinct from the morality of it.**

"Now I claim no exceptional expertise on any of this, but having worked at both the NSA and the CIA I do know a little bit about what I would consider to be lawful abuses. After all mass surveillance was argued to be constitutional, and yet the courts found very differently, despite

the fact that it was hidden and was occurring for more than a decade. A lawful abuse is something that I would define as an immoral or improper activity, perpetuated or justified under a shelter of law. Can you think of an example of that? I mean, it doesn't take long to look back in history and find them, I think, but what about things that are more recent.

"Mass surveillance of course is the example that's nearest to my own experience, but let's set that aside. What about torture? The Bush administration aggressively argued that torture could be legalized. What about indefinite detention? The internment of individuals for years without access to trial or due process. Extrajudicial killing. The targeted assassination of known individuals, far from any war zone, often by drone in today's world. Now they may be criminals. They may be even people who are armed combatants. In many cases, but not all. And the fact that these things are changing, often in secret, often without the public's awareness or their knowledge or consent should be disturbing, given that there are sort of covert legal protections for these encagements.

"Such abuses aren't limited strictly to National Security, and that is important, right, because we don't want this to entirely be this big paradigm of politics between, sort of, doves and hawks. **Segregation, slavery, genocides, these have all been perpetuated under frameworks that said they were lawful**, as long as you abided by the regulations that were sort of managing those activities.

"A lawful abuse of surveillance could also be more difficult to spot, not something that is as obvious. Or how about a restriction on who and how you can love someone, that's enforced by violence. Or something as simple as an intentional tax loophole. Or discrimination. Lawful abuse.

"So we've defined the term, right, but what is the actual problem. Well, advances in the quality of our technology, combined with the retreat in the quality of our legal frameworks have created paradigm, in which our daily activities produce an endless wealth of records, which can and are being used to do harm to individuals, including those who have themselves done no wrong. If you have a phone in your pocket that's turned on, a long-lived record of your movements has been created. As a result of the way the cell phone network functions. Your devices are constantly shouting into the air, by means of radio signals, a unique identity, that sort of validates you to the phone company. And this unique identity is not only saved by that phone company, but it can also be observed, as it travels through the air, by independent, even more dangerous, third parties.

"Due to the proliferation of sort of an ancient third party doctrine style interpretation of law, even the most predatory and unethical data collection regimes are often entirely legal. And effectively what this means is that **if you have a device, you have a dossier**. They may not be reading it, they may not be using it, but it's out there. Now, why should we care?

"Even if there are these comprehensive records being created about your private activities: where you are, who you went with, how long you were there, did you meet with anyone and so on and so forth, were any purchases made? Any sort of electronic activity record when these things are aggregated.

"I can think of 1,070 reasons why it matters. **According to the figures of the Committee to Protect Journalists, more than 1,070 journalists or media workers have been killed or gone missing since January of 2005**. This is something that might not be as intuitive as you might expect. People go, "well, we've had a lot of wars going on, surely it's combat related. These are combat deaths." But when you look at these same figures, murder is actually [a]

more common cause of death than combat. And amongst this number, politics was a more common newsbeat than war correspondence.

“Why is this? It’s because **one good journalist in the right place in the right time can change history**. One good journalist can move the needle in the context of an election. One good well-placed journalist can influence the outcome of a war. This makes them a target. And increasingly the tools of their trade are being used against them. Our technology is beginning to betray us, not just as individuals, but as classes of workers – particularly those putting a lot on the line, at risk, for the public interest. Speaking specifically here about journalists who by virtue of their trade rely upon communication in their daily work. And unfortunately, journalists are beginning to be targeted on the basis of specifically those communications.

“A single mistake can have a major impact. A single mistake can result in a detention, as was the case in the case of David Miranda, who was passing through London Heathrow actually, in the reporting that was relayed to me in my archive of material that was passed to journalists. His journalistic materials were seized by the British government. And this was after they intercepted communications regarding his plans to travel through their country.

“But it can also result in far, far worse than a detention. In the Syrian conflict the Assad regime began shelling the civilian city of Homs to an extent that almost all foreign journalists were forced to flee. Now, the government stopped accrediting journalists, and those who were accredited were reporting their locations were being harassed, they were being beaten, they were being disappeared. So only a handful remained, including a few who actually headed to this city, particularly to the Baba Amr district, to document the abuses that were being visit upon the population there.

“Typically in such circumstances, a journalist working in these kind of dangerous situations wouldn’t file their reports until after they had left the conflict area, because they don’t want to invite any kind of reprisal, it is dangerous. But what happens when you can’t wait. What happens when there are things that a government is sort of arguing aren’t happening and in fact are happening. The Syrian government at the time said, of course, that they weren’t targeting civilians, civilians weren’t being impacted. These were enemy combatants. And it’s important to understand that these lawful abuses of activities happen in many different places.

“You might be going, “oh, this is isn’t lawful. Surely this isn’t lawful.” And of course by an international law context you are absolutely right. By any sort of meaningful interpretation of the universal declaration of human rights this is a human rights violation, it is a war crime. But domestic laws are a hell of a thing. And you’ve got to remember that while you might trust American courts, China has courts, Russia has courts, North Korea has courts, Syria has courts, they have lawyers, they have offices of general council, who create policies to oversee and regulate these kind of activities and create frameworks to justify whatever it is that the institutions of power actually want to do.

“In this moment, in that Syrian city of Homs, the government was lying in a way that actually affected international relations. They were saying this was a justified offensive against enemy forces, and yet there was a reporter there by the name of Marie Colvin, who infiltrated the city. She actually crawled in, I believe, through a tunnel in the dark, had to climb stone walls and things like that. They couldn’t speak because they were afraid of being fired upon. And she said that this was not the case. She actually filed this report live despite the fact that they were worried that there might be some kind of government reprisal. She spoke four times to four different news agencies on a single day, and they sounded something like this:

[shows camera footage of Marie Colvin and her team in the Baba Amr district of Homs, Syria]

"This might sound like just another war story, but the next day the makeshift media centre that she was operating from, the one where the top floor had been hit the week before was repeatedly and precisely shelled by the Syrian army. She died as a result of this shelling, as did a French journalist. The photographer that she was working with was also wounded. It wasn't until sometime later that we found based on Lebanese signals intelligence collection and some other reporting, that the Syrian army had actually given the order to specifically target journalists, who were breaking sort of a news blackout in this organization.

"But how did they discover? How did they know where to aim their shells? According to reporting that occurred the week prior, I believe, her family has filed a lawsuit against the Syrian government. And they have evidence alleging that the radio frequency emissions of her communications, that she used to file those news reports, were intercepted by the Syrian army. They used direction finding capabilities to track and locate sort of this illegal, unlawful media center and then walk artillery fire toward it. Walking artillery fire is sort of how you re-aim artillery when it falls short or when it goes farther of where you're actually trying to hit. You have a spotter somewhere in the city who goes: "Oh you didn't quite hit the media center, you hit the hospital next door. Move it a little bit to the right, a little bit to the right. And they heard these shells coming.

"By the time the second shell hit, they knew they were in trouble. This happened at 6 o'clock in the morning. She was going to grab her shoes, because as is custom in the region you have to enter the house with bare feet. And she was caught by a shell and killed at that point. Now, there's a question here, among many policy officials, where they go: "was this legal? What processes do we use, to sort of remediate these kind of threats when these things happen? What happens when the policies fail?" And of course this is an argument that the Syrian government itself would say, it's "misunderstood." That "these were actually attacks by terrorists," or whatever, and "if we did these operations they were lawful," but there's a larger question of: does it matter?

"Does it matter whether it was authorized by law or not? Was this a moral action, regardless of whether it is lawful or unlawful. And: are these kind of things preventable? Can we enforce some stronger guarantee of the kind of locational indicators of our activities that we're putting out there. Perhaps in the case of Marie Colvin we could not. But what about the case of future journalists. What about a journalist who has to meet with source in a denied area. And they don't want their phone to be shouting into the air, to be giving up some kind of locational indicator of their movements.

"This is an area that is the focus of our research. Can we detect if the phone starts breaking the rules and, for example, if you turn off your wifi indicator, you put your phone in airplane mode, you try to turn off GPS. You get a little icon that lights up and says, "I'm off." But is that actually the case? Can you trust the device? What if the device has been hacked? What if something else is going on? So we wanted to investigate: can we use these same devices that are so frequently used against us, as a kind of canary, to detect these new targeted attempts for monitoring communications. Not just based on the emanations that go out on our phone, but malware attacks, intentional efforts to compromise the phone.

"For example: there was an Argentinean prosecutor, who, after he was murdered, when he was investigating whether the state had been engaged in serious violations of law, they recovered a mal-ware sample from his phone. Now that mal-ware sample did not match the operating system of his phone, so it was not responsible in that case, but it was clear that an

attempt had been made to compromise his devices and use them against him. This same malware was found targeting other activists, other journalists, other sort of lawyers in the Latin American region.

“If we can start to use devices, again, as a kind of canary to identify when these phones have been compromised, and we are able to get these to a targeted class of individuals, such as journalists, such as human rights workers, they can detect that these phones are breaking the rules, they’re acting in unexpected ways. What we can do, is we can begin affecting the risk calculation of the offensive actors in these cases.

“The NSA for example is very nervous about getting caught red handed. They don’t want to risk the political impact of being seen targeting groups like journalists, like American lawyers, despite the fact that they have been engaged in such operations. In rare cases, it’s not their meat and potatoes, but it does happen.

“Other governments are not so careful, but if we can create a track record of compromise, if we can create a track record of unlawful, of unethical activity, we can begin creating a framework to overturn the culture of impunity that affects so many of these lost journalists’ lives. In those 1,070 cases of dead journalists, or the disappeared, impunity was the most common outcome.

“But I want to make it clear here, that the idea is not just to protect an individual journalist’s phone, which is a worthy cause, but to, again, increase the costs of engaging in these kind of activities, engage in the costs of carrying out lawful abuses of digital surveillance, and without sort of belaboring the point here, let’s go to the actual technical side of this and talk about what we’ve actually done.”