

HBR Blog Network

I want to make one thing perfectly clear: this blog post is not an attack on the U.S., and my message is not anti-American. I have lived in the U.S. on and off for almost 12 years. I went to college in Boston (Berklee), my kids are both U.S. citizens as well as German citizens, and we have deep admiration for many American customs, traits, people and places.

But ever since 9/11, the U.S. government seems to have gone down a (until recently) secret path towards some kind of 'digital totalitarianism', with increasing disregard for other countries' mindsets and cultures.

The latest developments around PRISM and the NSA dragnet operations uncovered by Edward Snowden, in my view, severely damage the fragile fabric of the new global ecosystem, which we so sorely rely on in order to collectively tackle truly urgent global issues such as energy, pollution, food, climate change, (cyber-)terrorism and inequality.

Yes, of course, as more details about the NSA's mass surveillance activities are coming to light, it is also becoming clear that at least the other intelligence tribe members of UKUSA — i.e. the '5 Eyes' group (the U.S., the U.K., New Zealand, Australia, Canada) are pretty much doing the same thing, with Germany and France not far behind. But still: at the heart of this global collusion to Hoover up every bit of information about hundreds of millions of citizens under the pretense of fighting crime and terrorism sits the U.S. government, so let me start there.

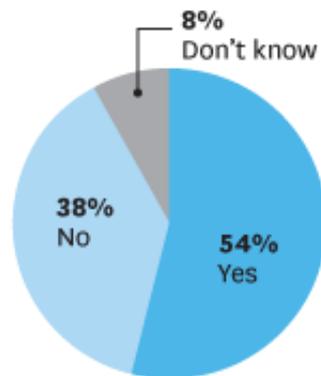
The past few weeks have been game-changing for the U.S./Europe relationship, with the EU Commission already hinting at moving cloud computing centers to Europe, many parliamentarians proposing to review international trade agreements and data exchange practices, and German chancellor Merkel heading towards a pre-election show-down on these very issues. It is not actually the fact that surveillance is real that scares Europeans, it is that now, everyone apparently is a legitimate target — yes we scan, because we can!

Little is being done by the U.S. government to address Europe's concerns, and most Americans seem to consider this whole affair a non-issue. (Granted, this sentiment may be **softening a bit**.) See the charts below:

MAJORITY OF AMERICANS SUPPORT SNOWDEN'S PROSECUTION

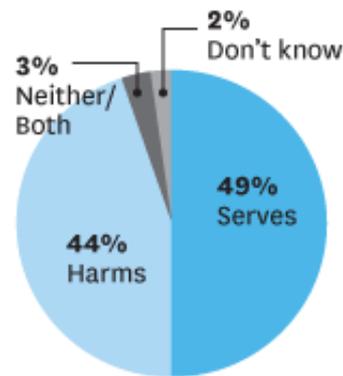
While the public opinion on Edward Snowden's leak is divided, the majority of those surveyed want him prosecuted.

Do you support Snowden's prosecution?



SOURCE PEW RESEARCH CENTER/USA TODAY

Does the NSA leak serve or harm public interest?



HBR.ORG

But, it is a big deal. And more people need to understand just how big.

For context, let's go back to 1788 and take a look at the words of James Madison, fourth president of the United States:

"There are more instances of the abridgment of the freedom of the people by gradual and silent encroachments of those in power than by violent and sudden usurpations."

The utter disrespect with which U.S. law enforcement agencies have violated the most basic international agreements on data security, basic citizens' rights and even diplomatic immunity is very worrisome, and will soon force people around the globe to rethink our relationship with 'all things USA' — whether it's President Obama and the U.S. government, or U.S.-based telecoms, technology companies and internet platforms such as Google, Apple, Microsoft, Facebook, Amazon, Yahoo and even Dropbox.

Meanwhile, President Obama seems happy to preside over this Orwellian affair with a newfound disregard for the basic privacy rights of citizens, which he previously expressed with great vigor back in 2005 and 2007, when he was still just a senator (watch these [NYT videos](#)). This is incredible — life is indeed stranger than fiction!

Let's be clear about this: for Europeans, in particular, the American shift towards state-sanctioned 'data totalitarianism' will have significant impact on whether we will

do business with U.S.-based companies that are in technology, media, cloud computing, social networking, telecommunications, e-commerce or 'big data', for they seemingly cannot do anything else than comply with the laws — and their extreme interpretations — as they are now (i.e. the [Patriot Act](#), [FISA courts](#), etc).

Therefore, some 50-75% of the worlds' largest digital communications and technology enterprises are now facing a seriously wicked dilemma: do they comply with FISA orders or do they protect their users (half of which are not even U.S. citizens)?

The bottom line is that currently all non-U.S. citizens seem to have no real protection, no recourse, no oversight... no power, and no rights. This is totally and utterly unacceptable and cannot be swept under the rug as 'business as usual'.

Sure, variations of the same plots are happening in China and in Russia, but who would have thought that the formerly alleged bastion of liberty and freedom, the United States of America, would resort to these sorts of global dragnet activities? This is wrong and that's all there is to it.

I believe that if this situation is not resolved very soon, non-U.S. internet users will be left with pretty much one option: some kind of a boycott or 'strike' — i.e. the explicit non-participation in those platforms and services that are subject to the totalitarian application of laws such as the U.S. Patriot Act.

The future of U.S.-based technology companies is at stake here, as is the future of U.S./EU relationships.

To remedy the situation, the leading U.S. internet and technology companies, led by Apple, Microsoft, Google, Yahoo and Facebook need to:

1. Unequivocally side with their real stakeholders — i.e. their users — and specifically assure us Europeans that they will act on our behalf, and seek to protect us against the abuse that has surfaced in the past few weeks.
2. Mount a strong campaign to urge President Obama and the U.S. Congress to stop these global mass surveillance activities, immediately, and put appropriate approval, remedy and redress mechanisms in place that are more in line with EU provisions, i.e. requiring actual cause for data surveillance activities, needing individual warrants, and informing the public on what the procedure is.
3. Urge the government to agree to a public trial of Edward Snowden that could

take place in a neutral location such as at the International Court of Justice in the Hague.

The U.S. government needs to:

1. Acknowledge the mistakes and rights violations that have occurred as far as the mass surveillance of global citizens are concerned, and uncover all additional instances. Dismissing the Director of National Intelligence (James Clapper) seems like another plausible step towards resolution, as well, given the fact that he pretty much lied to Congress.
2. Immediately discontinue the practice of spying on global citizens without individual warrants, and only in strict congruence with international laws and regulations.
3. Agree to a fair, public and open trial of Edward Snowden (see above).

If no action along these lines is taken, I think that the international community and hereto faithful users of American technologies and internet platforms will have no choice but to consider taking serious and possibly quite dramatic action to safeguard against this 'totalitarian surveillance creep'.

Some such actions for the international community may include:

1. Temporarily halting the [EU-US data exchange programs for travelers \(PNR and TFTP\)](#), which could potentially lead to a significant disruption of commercial air traffic between the U.S. and Europe (the review was already scheduled before the Snowden affair and is already in progress at the Commission).
2. Cut or significantly reduce ties with U.S.-based internet portals and service providers and shift business to providers based in other countries that are subject to international laws and explicit supervision (i.e. that can guarantee that appropriate processes and safeguards are in place). By extension, this would also concern the rest of the "5 Eyes" group, i.e. the UK, Canada, Australia and New Zealand.
3. Pause or even halt the current [Trans-Atlantic Free Trade Agreement](#) discussions until these demands, above, are met. Yes, I know, this could be quite painful for some EU countries but ... would they rather be 'collateral damage' now or take collective action to address potential long-term issues?
4. Open or expand cloud computing facilities in Europe (Luxembourg and Switzerland seem like good locations) and around the world. Until now, the

U.S.-based providers have dominated the global cloud business because of faster innovation and much larger investments in this sector — Europe needs to catch up urgently.

5. As global consumers, we just may need to stop using all U.S.-based services that won't voluntarily comply with international standards of data protection.
6. Offer a United Nations-supervised trial location and some kind of asylum to Edward Snowden, perhaps in the EU.

This is a game-changing moment, and it's time for global citizens to act. America: we love you, but enough is enough!