



Digital privacy from the economical pragmatic perspective



Digital privacy from the economical pragmatic perspective

3 digital privacy myths

1. Governments can effectively fight cybercrime
2. Every citizen has a right for digital privacy protection
3. Stricter regulations and legislation improve citizen's digital privacy

The government can effectively fight cybercrime

IT security investments should always make economical sense (if security investments exceed potential loss, implemented security countermeasures would be useless)

In the free security market, people pay for IT security solutions only if it makes economical sense or there is a risk of their reputation loss, otherwise it is just a waste of money

The government is unable to estimate security investments because...

- have no idea about threats in the private sector
- potential "reputation loss" has no real impact at all, as a monopoly institution, the government does not need reputation, therefore unable to perform a valid risk analysis
- have no idea if the given risk should be accepted or not
- if something does not work in the government (drug war, cybercrime war), it is because "it is underpaid" and it is "always necessary" to invest more tax-payers money
- if something does not work in the private sector, the company makes an economical decision - to remove the given service/product or to change it to be more productive



The government is unable to estimate security investments because...

- have no idea about threats in the private sector
- potential "reputation loss" has no real impact at all, as a monopoly institution the government does not need reputation, therefore unable to perform a valid risk analysis
- have no idea if the given risk should be accepted or not:
 - if something does not work in the government (drug war, cybercrime war), it is because "it is underpaid" and it is "always necessary" to invest more tax-payers money
 - if something does not work in the private sector, the company makes an economical decision - to remove the given service/ product or to change it to be more productive



The government is unable to estimate security investments because...

- have no idea about threats in the private sector
- potential "reputation loss" has no real impact at all, as a monopoly institution the government does not need reputation, therefore unable to perform a valid risk analysis
- have no idea if the given risk should be accepted or not:
 - if something does not work in the government (drug war, cybercrime war), it is because "it is underpaid" and it is "always necessary" to invest more tax-payers money
 - if something does not work in the private sector, the company makes an economical decision - to remove the given service/product or to change it to be more productive



YouTube



You Tube

"Leaking paradox"

- If any sensitive information is leaked from the private companies, they are obligated to pay penalties and their reputation is threatened (in the worst case they will bankrupt)
- If any sensitive information is leaked from the government institution (e.g. Slovak Cadaster), there is no risk of losing reputation (because of monopoly) and if the given institution pays any penalties, these penalties are always paid by tax-payers which leads to "leaking paradox":

Despite the fact that sensitive information of citizens are misused/leaked by the government, citizens are always those ones who will pay for their government's mistake.

Cybercrime is a
HYPE!

Despite the fact that loss caused by
cybercrime is apparently less than
government's investments, EU/US
budgets for fighting cybercrimes are
still increasing...
Ross Anderson, Chris Barton ... -
Measuring the Cost of Cybercrime.

Cybercrime is a HYPE!

Despite the fact that loss caused by cybercrime is apparently less than government's investments, EU/US budgets for fighting cybercrimes are still increasing...

Ross Anderson, Chris Barton .. -
Measuring the Cost of Cybercrime.

Every citizen has a right for digital privacy protection

- costs of the government privacy protection are always externalized to all tax-payers
- even those who do not care about their privacy and are not willing to contribute to that
- if you really care about privacy-ignoring people, invest your own money or time to education of these people, but do not force other people to pay for their digital privacy protection

You don't want to provide your
sensitive information to Facebook?
Don't use it, there are alternatives...
You don't want to provide your
sensitive information to Twitter?
Don't use it, there are alternatives...
You don't want to provide your
sensitive information to Google?
Don't use it, there are alternatives...



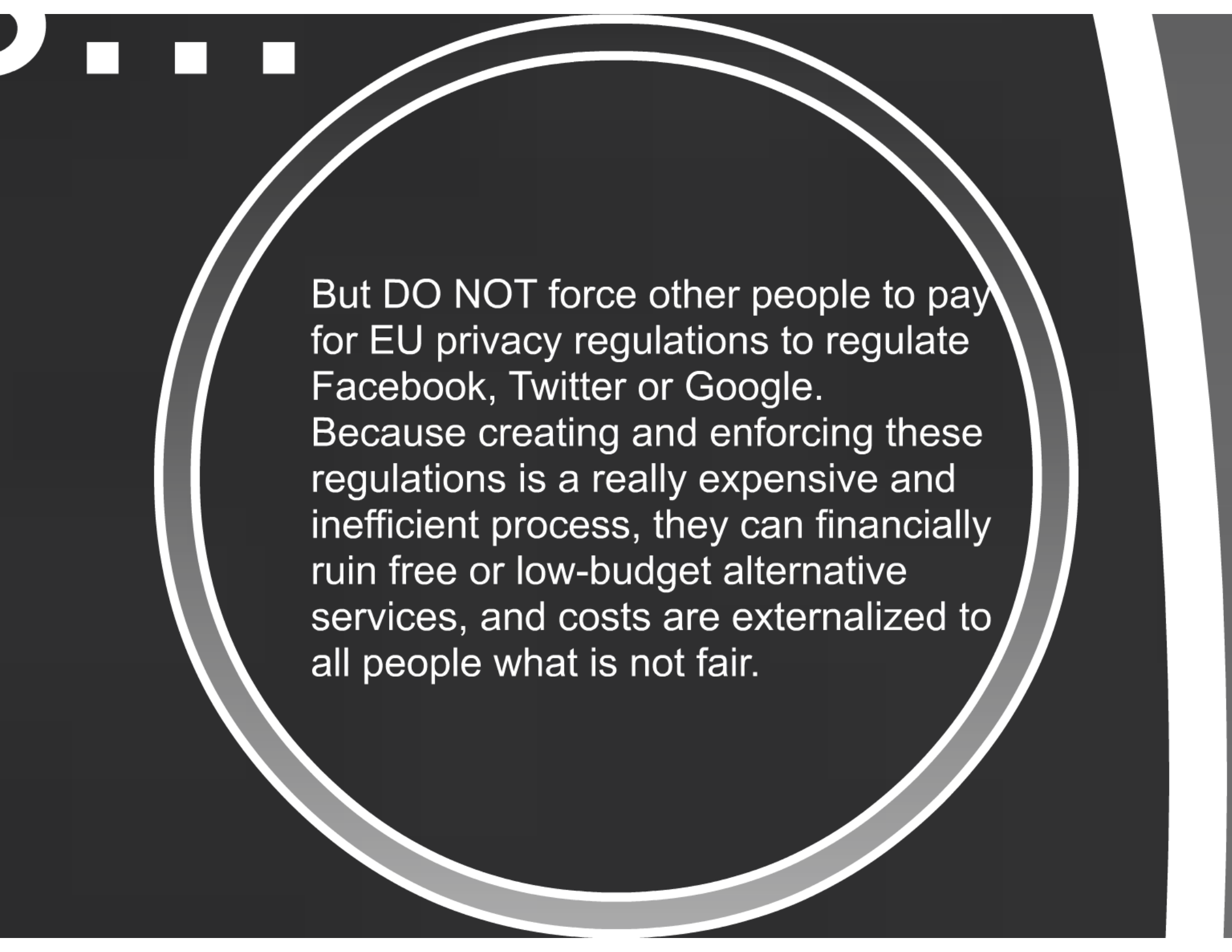
You don't want to provide your
sensitive information to Facebook?
Don't use it, there are alternatives...
You don't want to provide your
sensitive information to Twitter?
Don't use it, there are alternatives...
You don't want to provide your
sensitive information to Google?
Don't use it, there are alternatives...

But DO NOT force other people to pay
for EU privacy regulations to regulate
Facebook, Twitter or Google.
Because creating and enforcing these
regulations is a really expensive and
inefficient process. They can financially
run free or low-budget alternative
services, and costs are externalized to
all people who is not too.

But even irresponsible
people need a digital
privacy protection!

It is likely true, but if you always
care about them, they will be
always irresponsible...



A dark gray background featuring a large, light gray circle with a white outline. In the top left corner, there are three small white squares and a partial white circle. On the right side, there is a white diagonal line and a gray vertical bar.

But DO NOT force other people to pay
for EU privacy regulations to regulate
Facebook, Twitter or Google.
Because creating and enforcing these
regulations is a really expensive and
inefficient process, they can financially
ruin free or low-budget alternative
services, and costs are externalized to
all people what is not fair.

But even irresponsible
people need a digital
privacy protection!

It is likely true, but if you always
care about them, they will be
always irresponsible...

Ideal solution?

Everybody can decide
voluntarily if he wants to be a
product of Facebook, Google,
Twitter, ... and have these
services "for free"

or to be a customer of companies
that really care about digital
privacy and security and pay for
that

or use trusted open/
source alternatives

Ideal solution?

Everybody can decide voluntarily if he wants to be a product of Facebook, Google, Twitter, ... and have these services "for free"

or t
tha
priv
tha

on
so



or to be a customer of companies
that really care about digital
privacy and security and pay for
that



or use trusted open/
source alternatives

Stricter regulations and legislation will improve citizens' digital privacy

Stricter regulations almost always lead to better tracking and spying of innocent citizens:

- Data retention law (valid in the most EU countries)
- "Cash limits" valid in Slovakia and other EU countries (your payment information is always provided to 3rd party - your bank)
- PRISM-related spying programs
- All SWIFT payment transactions (sent to NSA)

Governments are the
biggest privacy threat

Anti-privacy regulations
are legally enforced and
directly supported by
your taxes



Governments are the
biggest privacy threat

Anti-privacy regulations
are legally enforced and
directly supported by
your taxes

Thanks a lot for your
attention!

