

# Privacy Protection: When Does Hiding in Plain Sight Work?

Tatiana Mayskaya<sup>1</sup> Arina Nikandrova<sup>2</sup>

<sup>1</sup>Higher School of Economics

<sup>2</sup>City, University of London

SEA, Miami

25 November 2019

## Privacy Debate

Protection against access of personal information:

## Privacy Debate

Protection against access of personal information:

- ▶ general protection (all information) — government / organization responsibility
  - ▶ ex: encryption of data in WhatsApp, US tradition of no trespassing signs
- ▶ selective protection (only sensitive information) — individual responsibility
  - ▶ ex: Royal family security protocols, one's habits on social media

# Privacy Debate

Protection against access of personal information:

- ▶ general protection (all information) — government / organization responsibility
  - ▶ ex: encryption of data in WhatsApp, US tradition of no trespassing signs
- ▶ selective protection (only sensitive information) — individual responsibility
  - ▶ ex: Royal family security protocols, one's habits on social media

Goal: protection of sensitive information

- ✗ General protection has high indirect cost since it limits access to big data

*Your individual data is actually not that valuable. While the entire data market might be worth \$3trn... it's access to huge aggregate data that is valuable.*

Privacy International

- ✓ Could providing tools for selective protection be a solution?

# Hiding in Plain Sight

## Take-away

When general protection is imperfect and perfect selective protection is infeasible, low selective protection (“hiding in plain sight”) becomes the optimal strategy for an individual even in the absence of protection cost. In other words, when perfect selective protection is infeasible, **general and selective protections are complements.**

## Policy implication

Tools that facilitate selective protection might not be used in practice in the absence of good general protection.

# Hiding in Plain Sight

## Take-away

When general protection is imperfect and perfect selective protection is infeasible, low selective protection (“hiding in plain sight”) becomes the optimal strategy for an individual even in the absence of protection cost. In other words, when perfect selective protection is infeasible, **general and selective protections are complements.**

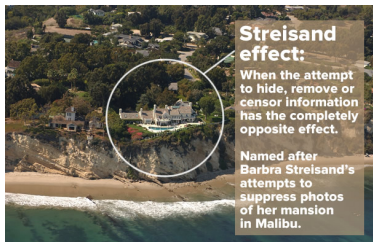
## Policy implication

Tools that facilitate selective protection might not be used in practice in the absence of good general protection.

## High-Level Intuition

By lowering selective protection, an individual incentivizes the following logic for an invader: “Had there anything interesting to find, I would have found it already, so I give up”

## Example: Streisand Effect



### Streisand Effect

Barbra Streisand failed to take into account the indirect cost of increasing selective protection: stronger protection attracts more attention.

# Model

- ▶ The game is between a celebrity and a journalist.
- ▶ The celebrity publicly commits to the level of **selective protection** parametrized by  $\mu_1 > 0$ .
  - ▶ useful connections, advocates, loopholes in protocols, options to remove parts of own digital fingerprint, installed VPN service, etc  $\Rightarrow$  tools that the celebrity would use if and only if a story that compromises her happens



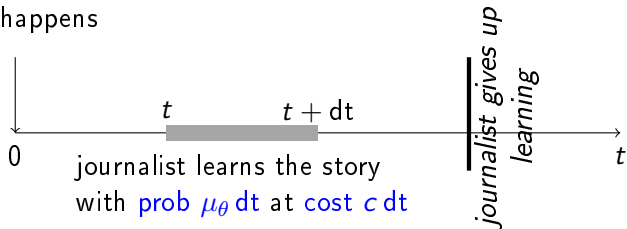
# Model

- ▶ The game is between a celebrity and a journalist.
- ▶ The celebrity publicly commits to the level of **selective protection** parametrized by  $\mu_1 > 0$ .
- ▶ A story that draws the journalist's attention happens. It could be either compromising ( $\theta = 1$ ) or not interesting ( $\theta = 0$ ). The **probability it is compromising** is  $p \in (0, 1)$ .
  - ▶ exogenous  $\Rightarrow$  independent of ex post protection; no ex ante signaling through protection level
  - ▶ interpretations of  $p$ : publicly observable ability of a journalist to detect an interesting story; type of the celebrity reflecting her propensity to get involved in a scandal

## Model

- ▶ The game is between a celebrity and a journalist.
- ▶ The celebrity publicly commits to the level of **selective protection** parametrized by  $\mu_1 > 0$ .
- ▶ A story that draws the journalist's attention happens. It could be either compromising ( $\theta = 1$ ) or not interesting ( $\theta = 0$ ). The **probability it is compromising** is  $p \in (0, 1)$ .

story happens



- ▶  $\mu_0 > 0$  characterizes **general protection**
- ▶ If the journalist knows the story, he can report it. Once he reports the story he gets  $\beta > 0$  if  $\theta = 1$  and some negative payoff otherwise.
- ▶ The celebrity minimizes the probability of a report

## Beliefs

As long as the journalist searches and does not find the story, his belief  $p_t$  about  $\theta = 1$

(D) drifts down when  $\mu_1 > \mu_0$  (selective protection is less than general protection)

(C) stay constant when  $\mu_1 = \mu_0$

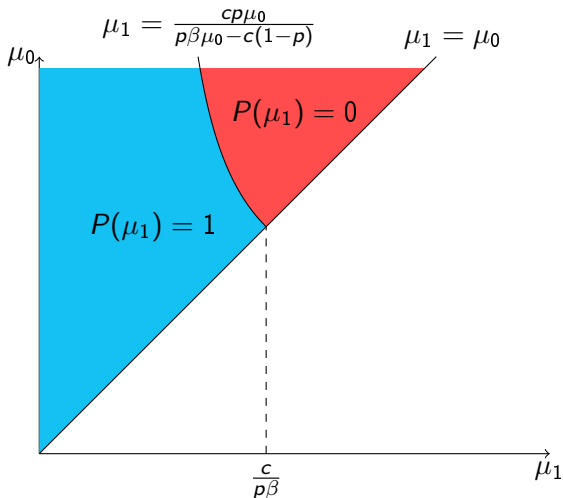
(U) drifts up when  $\mu_1 < \mu_0$

$$\left( \ln \frac{p_t}{1 - p_t} \right)'_t = \mu_0 - \mu_1$$

(C)+(U): Expected benefit from learning until the story is found:

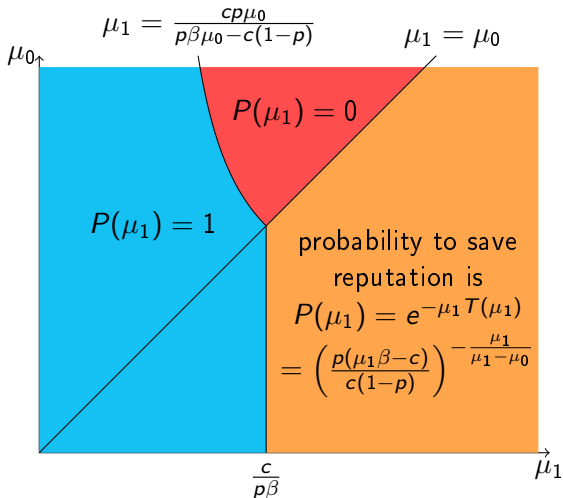
$$V(\mu_1) = p\beta - \frac{cp}{\mu_1} - \frac{c(1-p)}{\mu_0}$$

Full protection  $\Leftrightarrow V(\mu_1) \leq 0 \Leftrightarrow \mu_1 (p\beta\mu_0 - c(1-p)) \leq cp\mu_0$ .

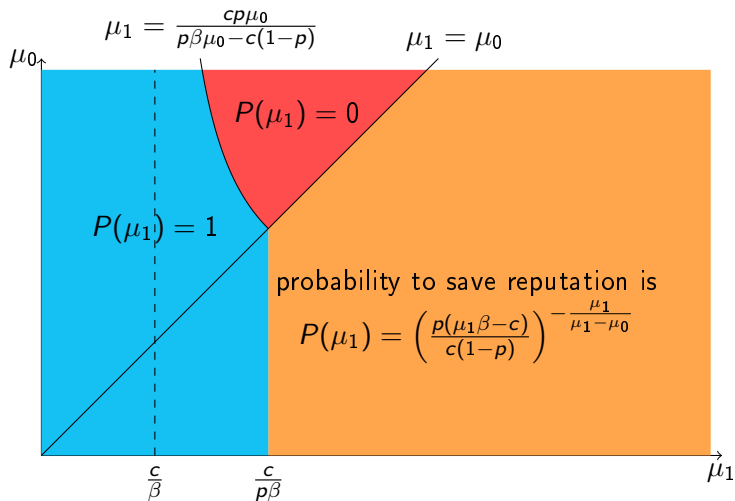


(D): The optimal stopping time in the absence of finding:

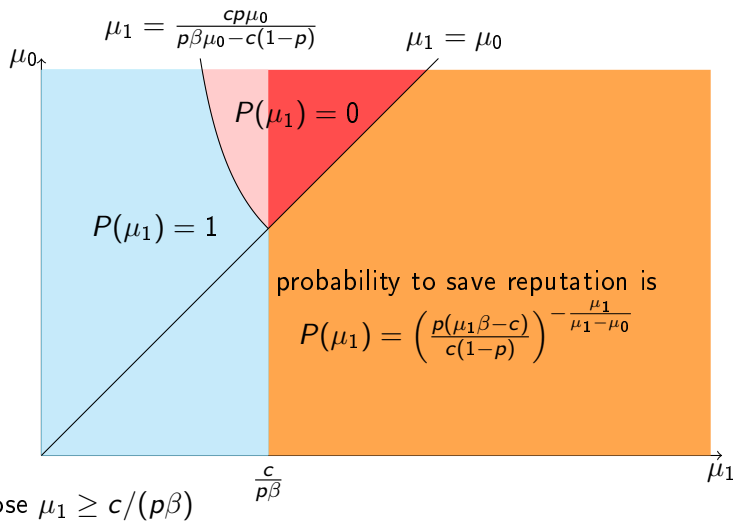
$$T(\mu_1) = \begin{cases} \frac{1}{\mu_1 - \mu_0} \ln \left( \frac{\rho(\mu_1\beta - c)}{c(1-\rho)} \right), & \mu_1 > \frac{c}{\rho\beta} \\ 0, & \mu_1 \leq \frac{c}{\rho\beta} \end{cases}$$



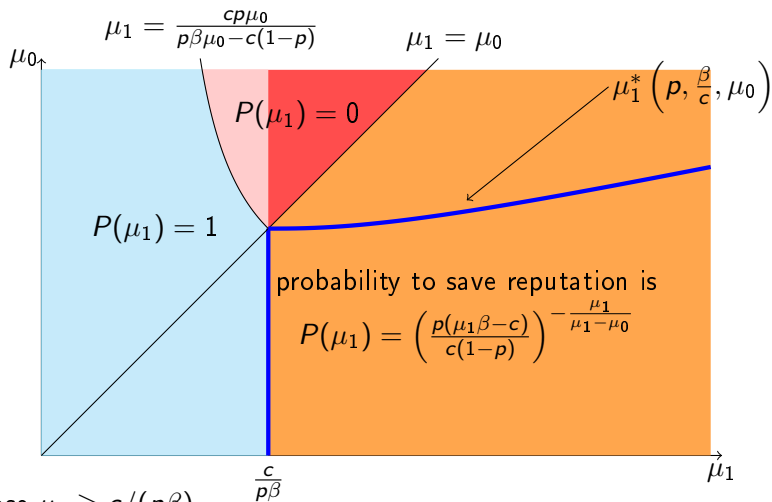
# Optimal Selective Protection



# Optimal Selective Protection



# Optimal Selective Protection



suppose  $\mu_1 \geq c/(p\beta)$

- ▶ if  $\mu_0 < c/(p\beta)$ , then  $\mu_1^* = c/(p\beta)$
- ▶ if  $\mu_0 > c/(p\beta)$ , then  $\mu_1^* \left( p, \beta/c, \mu_0 \right) > \mu_0$



## Trade-Off

$$P(\mu_1) = \left( \frac{p(\mu_1\beta - c)}{c(1-p)} \right)^{-\frac{\mu_1}{\mu_1 - \mu_0}}$$

- ▶ search cost:

$$\uparrow c \sim \downarrow \mu_1 \Rightarrow \uparrow \underline{p} = \min \left\{ \frac{c}{\mu_1\beta}, p \right\} \Rightarrow \uparrow P(\mu_1)$$

- ▶ speed of learning:

$$\downarrow \mu_1 \Rightarrow \downarrow \dot{q}_t = \left( \ln \frac{1-p_t}{p_t} \right)'_t = \mu_1 - \mu_0 \Rightarrow \downarrow P(\mu_1)$$

- ▶ speed of revelation:

$$\downarrow \mu_1 \Rightarrow \uparrow P(\mu_1)$$

## Examples: *Twilight* (2008)


*Sometimes the best hiding place is the one that's in plain sight.*  
Stephenie Meyer



A vampire family was hiding in plain sight (e.g. go to school) all along and nobody figured that out...

## Examples: Anti-Corruption Foundation in Russia

- ▶ since 2011 ACF accused of corruption more than 50 Russian government officials
- ▶ staff includes only 30 people
- ▶ have access only to publicly available data



ФОНД БОРЬБЫ  
С КОРРУПЦИЕЙ

Why does government provide so little protection for their own?

- ▶ almost all government officials in Russia are corrupt.
- ▶ the most corrupt officials are also members of the elite “club” that has government as their “krysha”
- ▶ low “general” protection for government officials outside of the “club” ⇒ low protection for their own

A close-up portrait of Benedict Cumberbatch as Sherlock Holmes, looking slightly to the right with a serious expression. The background is dark with a bright, out-of-focus circular light source on the right side. The quote is overlaid in white, bold, sans-serif text.

**SAFEST  
PLACE  
TO HIDE,  
IS IN  
PLAIN SIGHT.**

**- Sherlock Holmes**

#Sherlock

theQuotes.me