Privacy Protection: When Does Hiding in Plain Sight Work?

Tatiana Mayskaya[1] Arina Nikandrova[2]

[1]Higher School of Economics

[2]City, University of London

Microeconomics Workshop
ICEF-HSE
31 October 2019

Tutankhamun Tomb

- In 1922, Howard Carter discovered the tomb of young pharaoh Tutankhamun
- This tomb is too small for a royal and was originally intended for somebody else
- Up to date, this remains the only pharaoh tomb in the Valley of the Kings that was found nearly intact

When Does Hiding in Plain Sight Work?

Trade-off: *intensity* vs *longevity*

- strong protection ⇒ hard to find ⇒ low intensity of search
- weak protection ⇒ quickly become pessimistic about finding anything ⇒ low longevity of search

When Does Hiding in Plain Sight Work?

Trade-off: *intensity* vs *longevity*

- strong protection ⇒ hard to find ⇒ low intensity of search
- weak protection ⇒ quickly become pessimistic about finding anything ⇒ low longevity of search

Examples:

- company hiding its bad financial performance from the market
- corrupt politician hiding her manipulations from public
- celebrity hiding her private life from paparazzi

When Does Hiding in Plain Sight Work?

Trade-off: *intensity* vs *longevity*

- strong protection ⇒ hard to find ⇒ low intensity of search
- weak protection ⇒ quickly become pessimistic about finding anything ⇒ low longevity of search

Examples:

- company hiding its bad financial performance from the market
- corrupt politician hiding her manipulations from public
- celebrity hiding her private life from paparazzi

Common elements:

- **one + many**: single entity (*celebrity*) aims to prevent multiple agents (*paparazzi*) from uncovering a sensational story about her
- **ex ante uncertainty**: story could be either sensational or not
- **exclusivity**: each paparazzi benefits only from reporting previously unpublished sensational stories

Model

Players: celebrity and *n* paparazzi

- Celebrity commits to privacy policy $\{\lambda_1, \lambda_0\}$

Model

Players: celebrity and *n* paparazzi

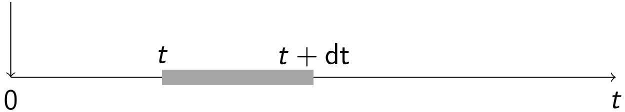
- Celebrity commits to privacy policy $\{\lambda_1, \lambda_0\}$
- Celebrity gets involved in a story which is either sensational ($\theta = 1$) or not ($\theta = 0$); story type θ remains private to celebrity
- Let *p* be probability that $\theta = 1$

Model

Players: celebrity and n paparazzi

- Celebrity commits to privacy policy $\{\lambda_1, \lambda_0\}$
- Celebrity gets involved in a story which is either sensational ($\theta = 1$) or not ($\theta = 0$); story type θ remains private to celebrity
- Let p be probability that $\theta = 1$

story happens

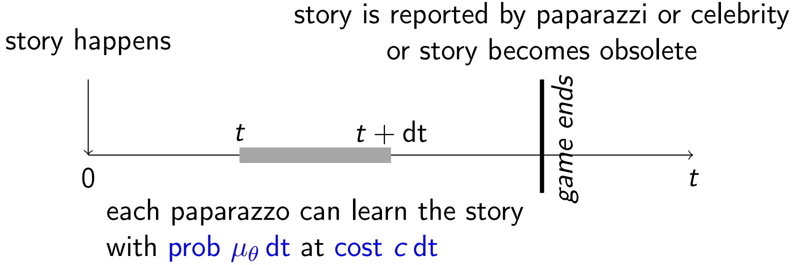


each paparazzo can learn the story
with prob μ_θ dt at cost c dt

Model

Players: celebrity and n paparazzi

- Celebrity commits to privacy policy $\{\lambda_1, \lambda_0\}$
- Celebrity gets involved in a story which is either sensational ($\theta = 1$) or not ($\theta = 0$); story type θ remains private to celebrity
- Let p be probability that $\theta = 1$

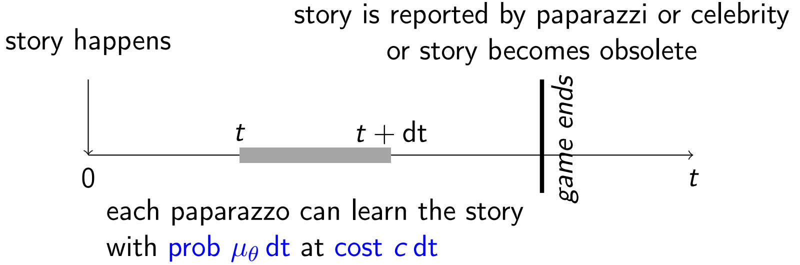


- Paparazzo can report the story only if he knows it
- Celebrity reveals the story to all actively searching paparazzi at rate λ_θ
- Story becomes obsolete at rate ρ

Model

Players: celebrity and n paparazzi

- Celebrity commits to privacy policy $\{\lambda_1, \lambda_0\}$
- Celebrity gets involved in a story which is either sensational ($\theta = 1$) or not ($\theta = 0$); story type θ remains private to celebrity
- Let p be probability that $\theta = 1$



- Paparazzo can report the story only if he knows it
- Celebrity reveals the story to all actively searching paparazzi at rate λ_θ
- Story becomes obsolete at rate ρ
- Reports are public, learning is private

Payoffs

- Paparazzo gets (apart from learning cost)

$$\begin{cases} \beta - \phi > 0, & \text{if reports unpublished up-to-date sensational story} \\ -\phi < 0, & \text{if reports published, or obsolete,} \\ & \qquad\qquad \text{or not sensational story} \\ 0, & \text{if never reports or celebrity reveals the story herself} \end{cases}$$

Payoffs

- Paparazzo gets (apart from learning cost)

$$\begin{cases} \beta - \phi > 0, & \text{if reports unpublished up-to-date sensational story} \\ -\phi < 0, & \text{if reports published, or obsolete,} \\ & \qquad\qquad\qquad \text{or not sensational story} \\ 0, & \text{if never reports or celebrity reveals the story herself} \end{cases}$$

- Celebrity wants to minimize the probability the sensational story being reported (either by herself or paparazzi) before it becomes obsolete
  NB: Assume protection is costless

Learning Pattern

While the game continues:

- sensational story

Learning Pattern

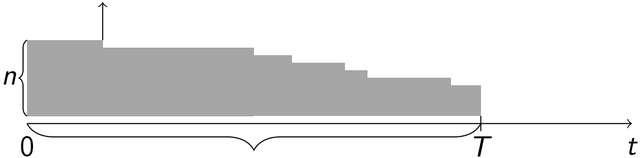
While the game continues:

- sensational story

nobody knows the story;
all paparazzi invest in learning

- non-sensational story

paparazzo *i* learns the story



all paparazzi who do not know the story
invest in learning

Beliefs

$$\text{no finding} \quad \Rightarrow \quad \begin{cases} p_t(1 - a_1\,\mathrm{dt}) & \theta = 1 \text{ \& learning continues} \\ (1 - p_t)(1 - a_0\,\mathrm{dt}) & \theta = 0 \text{ \& learning continues} \end{cases}$$

where

$$a_1 = n\mu_1 + \lambda_1 + \rho$$
$$a_0 = \mu_0 + \lambda_0 + \rho$$

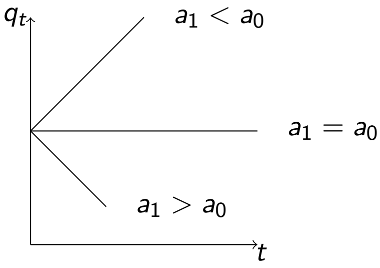
Beliefs

$$\text{no finding} \quad \Rightarrow \quad \begin{cases} p_t(1 - a_1\,\mathrm{dt}) & \theta = 1 \text{ \& learning continues} \\ (1-p_t)(1 - a_0\,\mathrm{dt}) & \theta = 0 \text{ \& learning continues} \end{cases}$$

$$\Rightarrow \quad \dot{q}_t \equiv \left(\ln \frac{p_t}{1-p_t}\right)'_t = -(a_1 - a_0)$$

where

$$a_1 = n\mu_1 + \lambda_1 + \rho$$
$$a_0 = \mu_0 + \lambda_0 + \rho$$



Modeling Privacy Policy: Discussion

$$\dot{q}_t = -(a_1 - a_0), \quad a_1 = n\mu_1 + \lambda_1 + \rho, \quad a_0 = \mu_0 + \cancel{\lambda_0}^{\,0} + \rho$$

Observation 1

The more pessimistic the paparazzi are about $\theta = 0$ (the lower q_t), the better off the celebrity is $\Rightarrow$ $\lambda_0 = 0$ is optimal

Modeling Privacy Policy: Discussion

$$\dot{q}_t = -(a_1 - a_0), \quad a_1 = n\mu_1 + \lambda_1 + \rho, \quad a_0 = \mu_0 + \cancel{\lambda_0}^{\,0} + \rho$$

Observation 1

The more pessimistic the paparazzi are about $\theta = 0$ (the lower q_t), the better off the celebrity is $\Rightarrow$ $\lambda_0 = 0$ is optimal

Observation 2

n and λ_1 enter only as $n\mu_1 + \lambda_1$ $\Rightarrow$ choosing λ_1 is equivalent to choosing n

In reality, protection could be of two types:

1. Limit access (build higher "fence") $\Rightarrow$ decrease n
2. Control own behavior (build stronger "fence") $\Rightarrow$ decrease λ_1

Modeling Privacy Policy: Discussion

$$\dot{q}_t = -(a_1 - a_0), \quad a_1 = n\mu_1 + \lambda_1 + \rho, \quad a_0 = \mu_0 + \cancel{\lambda_0}^{\,0} + \rho$$

Observation 1

The more pessimistic the paparazzi are about $\theta = 0$ (the lower q_t), the better off the celebrity is $\Rightarrow$ $\lambda_0 = 0$ is optimal

Observation 2

n and λ_1 enter only as $n\mu_1 + \lambda_1$ $\Rightarrow$ choosing λ_1 is equivalent to choosing n

In reality, protection could be of two types:

1. Limit access (build higher "fence") $\Rightarrow$ decrease n
2. Control own behavior (build stronger "fence") $\Rightarrow$ decrease λ_1

NB: Celebrity unambiguously wants c to be high. Assume she has no control over c

Modeling Privacy Policy: Discussion

$$\dot{q}_t = -(a_1 - a_0), \quad a_1 = n\mu_1 + \lambda_1 + \rho, \quad a_0 = \mu_0 + \cancelto{0}{\lambda_0} + \rho$$

Observation 1

The more pessimistic the paparazzi are about $\theta = 0$ (the lower q_t), the better off the celebrity is $\Rightarrow$ $\lambda_0 = 0$ is optimal

Observation 2

n and λ_1 enter only as $n\mu_1 + \lambda_1$ $\Rightarrow$ choosing λ_1 is equivalent to choosing n

In reality, protection could be of two types:

1. Limit access (build higher "fence") $\Rightarrow$ decrease n
2. Control own behavior (build stronger "fence") $\Rightarrow$ decrease λ_1

NB: Celebrity unambiguously wants c to be high. Assume she has no control over c

Observation 3

When $a_1 \leq a_0$, learning never stops if it is ever optimal $\Rightarrow$ $a_1 > a_0$ is optimal

Observation 4

If

$$\underbrace{c}_{\text{flow cost of learning}} \geq \underbrace{p\mu_1(\beta - \phi)}_{\text{flow benefit of learning when } a_1 = a_0}$$

then the celebrity could make $T = 0$ *and save her reputation for sure by choosing* $a_1 > a_0$*.*

Observation 4

If

$$\underbrace{c}_{\textit{flow cost of learning}} \geq \underbrace{p\mu_1(\beta - \phi)}_{\textit{flow benefit of learning when } a_1 = a_0}$$

then the celebrity could make $T = 0$ and save her reputation for sure by choosing $a_1 > a_0$.

Assumption 1

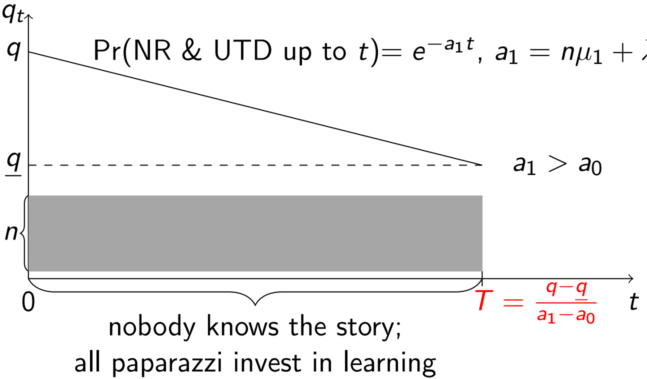
$c < p\mu_1(\beta - \phi)$

Celebrity sets $a_1 > a_0$ in equilibrium $\Rightarrow$ p_t drifts down until $\underline{p} = \frac{c}{\mu_1(\beta - \phi)}$

Celebrity saves her reputation with probability

$$\underbrace{\int_0^T \rho e^{-a_1 t}\,\mathrm{dt}}_{\text{story gets obsolete while paparazzi learn}} + \underbrace{e^{-a_1 T}}_{\text{story gets obsolete after paparazzi stop}}$$

sensational story: *conditional on no report (NR) & up-to-date story (UTD)*



NB: $q = \ln \frac{p}{1-p}$, $\underline{q} = \ln \frac{\underline{p}}{1-\underline{p}}$, $\underline{p} = \frac{c}{\mu_1(\beta - \phi)}$ do not depend on a_1 and a_0

Intensity vs Longevity Trade-off

Celebrity maximizes

$$\max_{a_1} \quad P(a_1, T(a_1)) = \int_0^{T(a_1)} \rho e^{-a_1 t}\,\mathrm{dt} + e^{-a_1 T(a_1)}$$

$$\frac{dP(a_1, T(a_1))}{da_1} = \underbrace{\frac{\partial P(a_1, T)}{\partial a_1}}_{\substack{<0 \\ \text{intensity}}} + \underbrace{\frac{\partial P(a_1, T)}{\partial T}\frac{dT(a_1)}{da_1}}_{\substack{>0 \\ \text{longevity}}}$$

$$T(a_1) = \frac{q - \underline{q}}{a_1 - a_0} \quad \Rightarrow \quad \frac{dT(a_1)}{da_1} < 0$$

Intensity vs Longevity Trade-off

Celebrity maximizes

$$\max_{a_1} \quad P(a_1, T(a_1)) = \int_0^{T(a_1)} \rho e^{-a_1 t}\,\mathrm{dt} + e^{-a_1 T(a_1)}$$

$$\frac{dP(a_1, T(a_1))}{da_1} = \underbrace{\frac{\partial P(a_1, T)}{\partial a_1}}_{\substack{<0 \\ \text{intensity}}} + \underbrace{\frac{\partial P(a_1, T)}{\partial T}\frac{dT(a_1)}{da_1}}_{\substack{>0 \\ \text{longevity}}}$$

$$T(a_1) = \frac{q - \underline{q}}{a_1 - a_0} \quad \Rightarrow \quad \frac{dT(a_1)}{da_1} < 0$$

NB: n and λ_1 affect $a_1 = n\mu_1 + \lambda_1 + \rho$ but not $\underline{q} = \ln \frac{\underline{p}}{1-\underline{p}}$, $\underline{p} = \frac{c}{\mu_1(\beta-\phi)}$

Intensity vs Longevity Trade-off

Celebrity maximizes

$$\max_{a_1} \quad P(a_1, T(a_1)) = \int_0^{T(a_1)} \rho e^{-a_1 t}\, \mathrm{dt} + e^{-a_1 T(a_1)}$$

$$\frac{dP(a_1, T(a_1))}{da_1} = \underbrace{\frac{\partial P(a_1, T)}{\partial a_1}}_{\substack{<0 \\ \text{intensity}}} + \underbrace{\frac{\partial P(a_1, T)}{\partial T}\frac{dT(a_1)}{da_1}}_{\substack{>0 \\ \text{longevity}}}$$

$$T(a_1) = \frac{q - \underline{q}}{a_1 - a_0} \quad \Rightarrow \quad \frac{dT(a_1)}{da_1} < 0$$

NB: n and λ_1 affect $a_1 = n\mu_1 + \lambda_1 + \rho$ but not $\underline{q} = \ln \frac{\underline{p}}{1-\underline{p}}$, $\underline{p} = \frac{c}{\mu_1(\beta-\phi)}$

<u>Ex post</u> *neither celebrity nor paparazzi get positive benefit from "leaks" (λ_1) or competition (n). In fact, celebrity is hurt by them.*

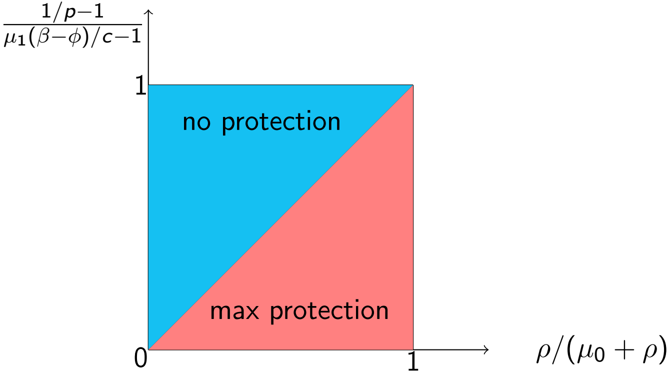
<u>Ex ante</u> *they serve as a commitment device for celebrity, which, together with uncertainty about $\theta = 1$, incentivizes paparazzi to give up earlier*

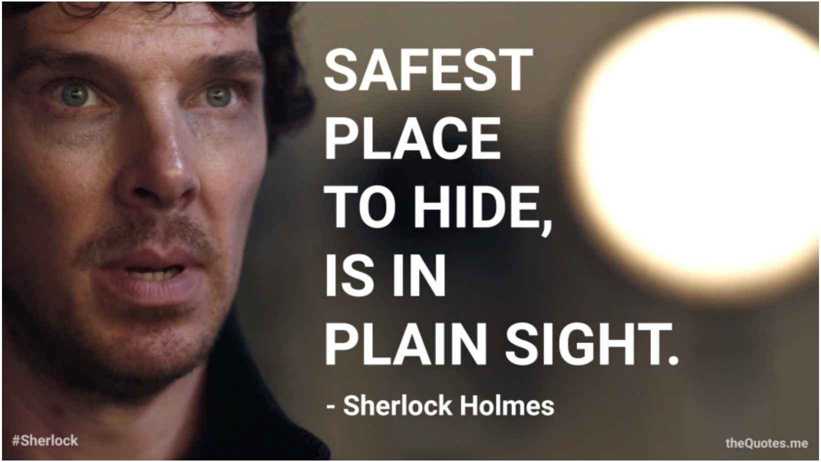
Theorem 1

Either $a_1 = a_0$ or $a_1 = +\infty$ is optimal. The celebrity saves her reputation with probability

$$\lim_{a_1 \to a_0} P(a_1) = \frac{\rho}{a_0}, \quad a_0 = \mu_0 + \rho$$

$$\lim_{a_1 \to +\infty} P(a_1) = \frac{\underline{p}(1-p)}{p(1-\underline{p})}, \quad \underline{p} = \frac{c}{\mu_1(\beta - \phi)}$$




SAFEST
PLACE
TO HIDE,
IS IN
PLAIN SIGHT.
- Sherlock Holmes
#Sherlock
theQuotes.me