The UK is trying to colonize the internet

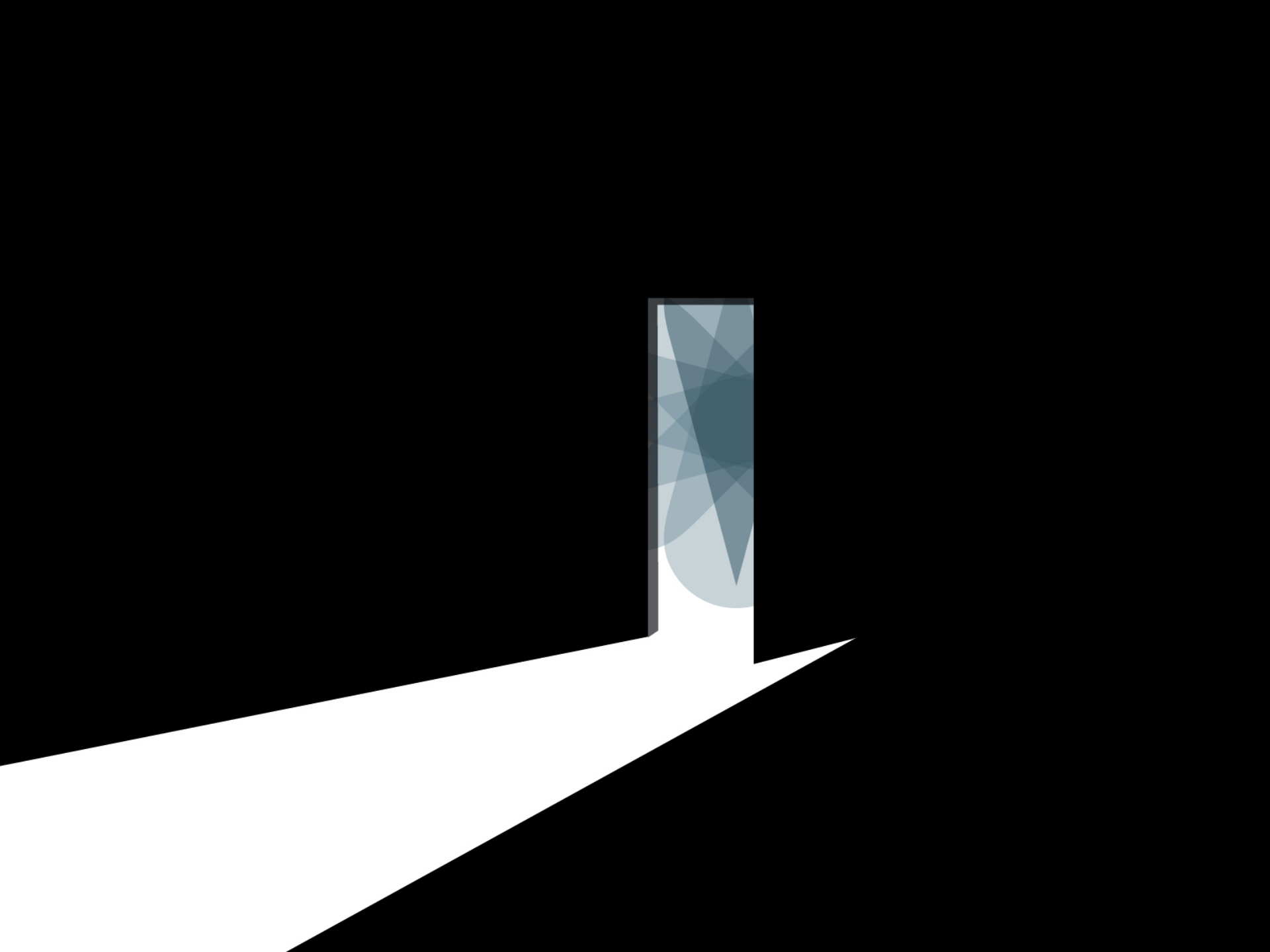
AND OTHER SCARY CRYPTO TALES TO TELL IN THE DARK

AMIE STEPANOVICH | U.S. POLICY MANAGER

AMIE@ACCESSNOW.ORG

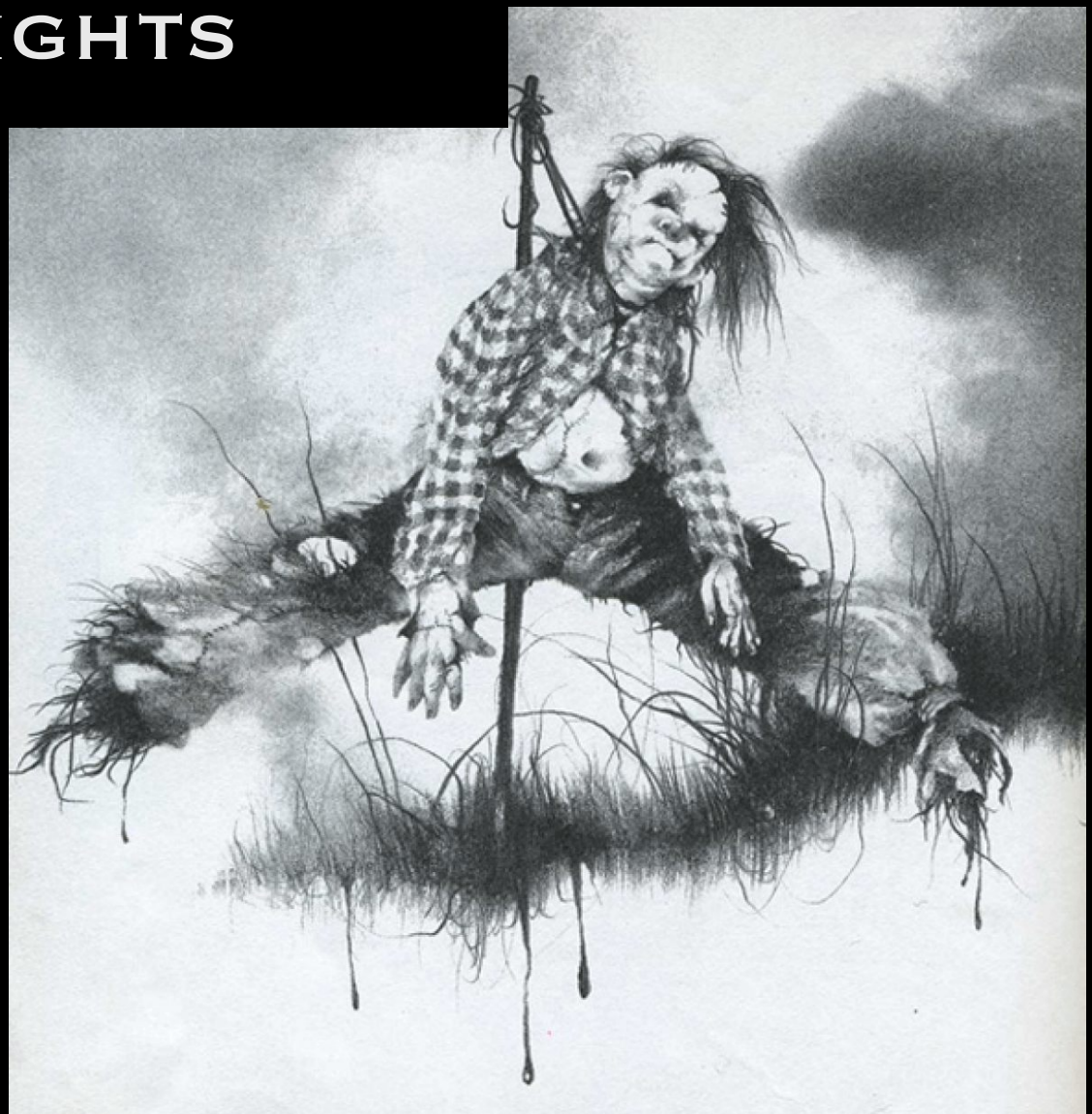
accessnow

accessnow



This security stuff...it's hard!

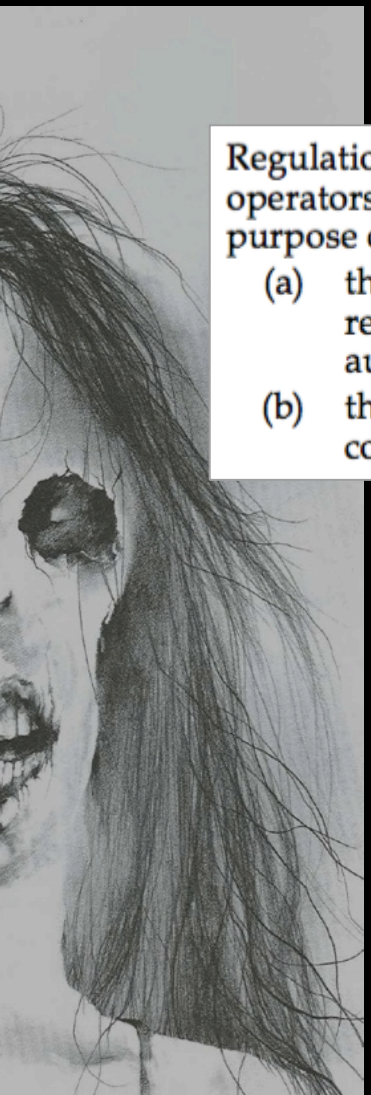
Undermining encryption harms human rights

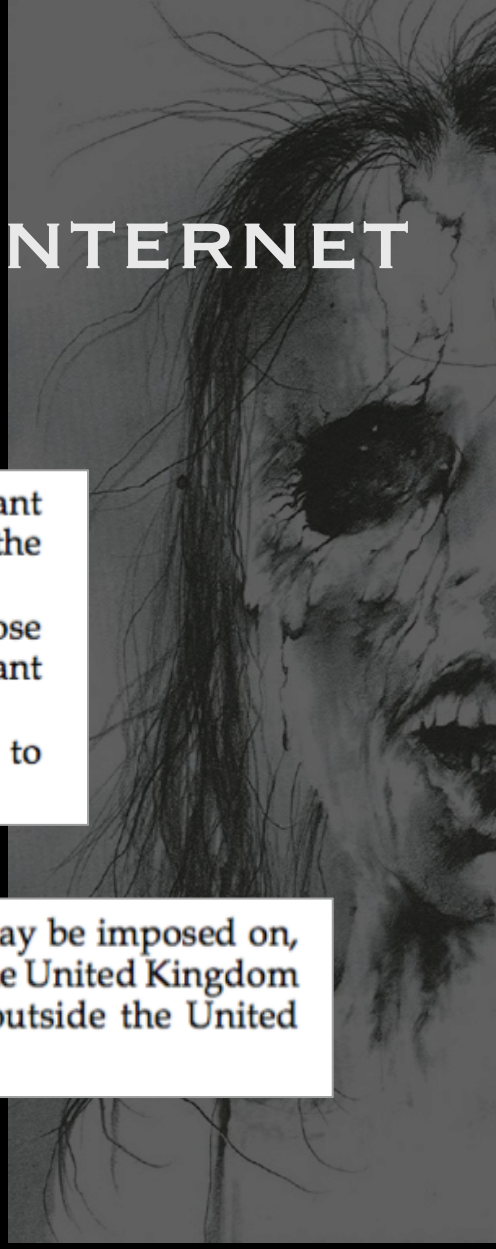


Back doors, and key escrow, and bans (oh my)

- Ban encryption
- Backdoors and vulnerabilities
- Key escrow
- Undermining standards
- Mandating standards
  or algorithms
- Pressuring companies

The UK wants to pwn the internet





Regulations under this section may impose an obligation on any relevant operators only if the Secretary of State considers it is reasonable to do so for the purpose of securing—

(a) that it is (and remains) practicable to impose requirements on those relevant operators to provide assistance in relation to relevant authorisations (see subsection (9)), and

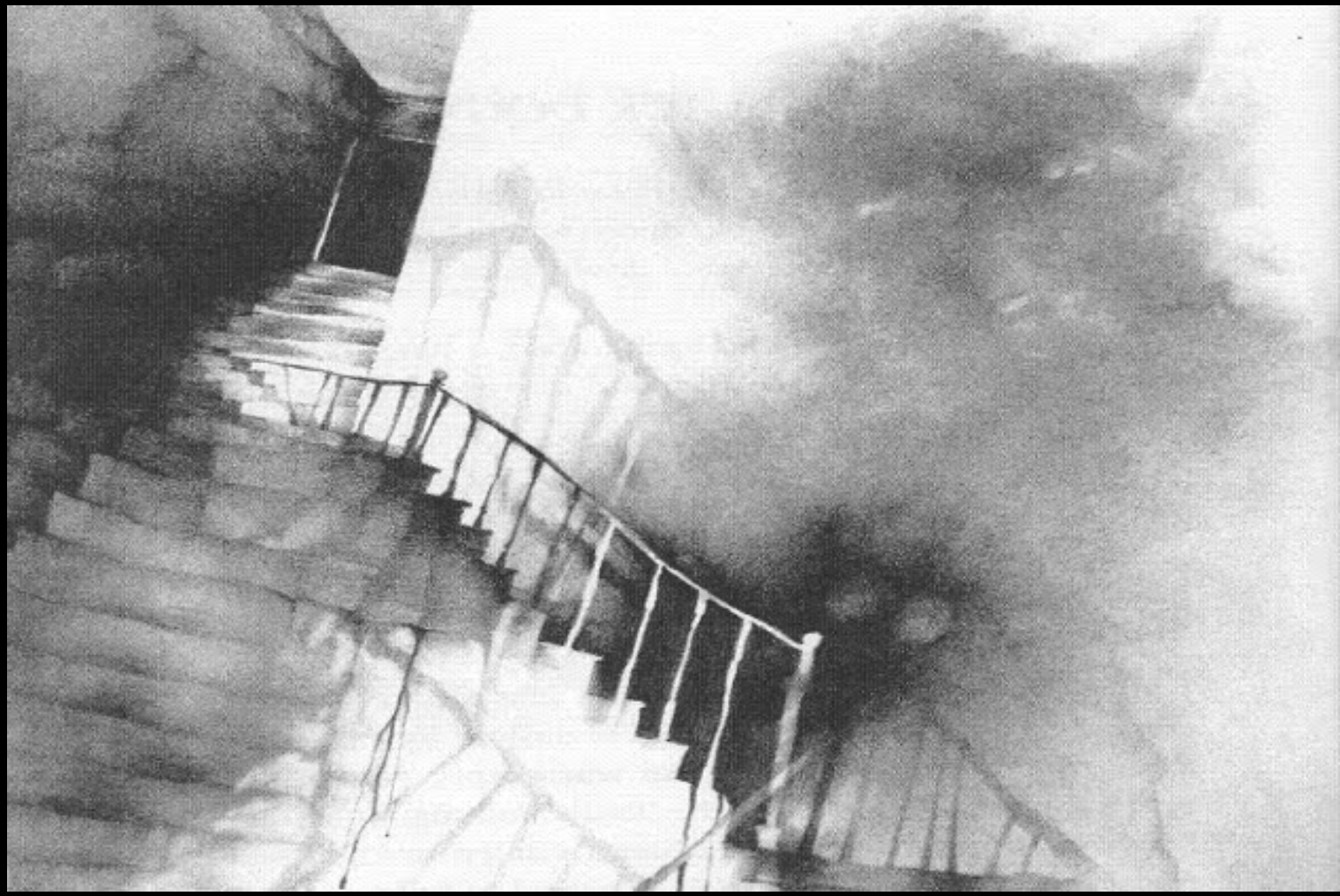
(b) that it is (and remains) practicable for those relevant operators to comply with those requirements.

An obligation specified in regulations under this section may be imposed on, and a technical capability notice given to, persons outside the United Kingdom (and may require things to be done, or not to be done, outside the United Kingdom).

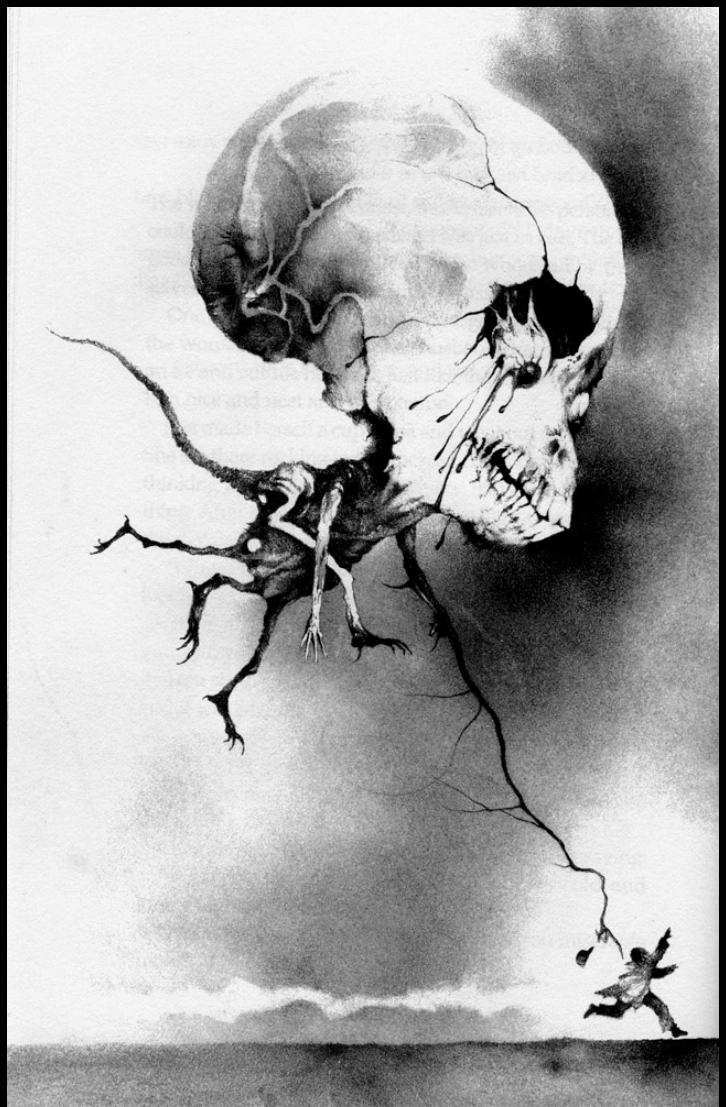
This takes us down a “dark” path

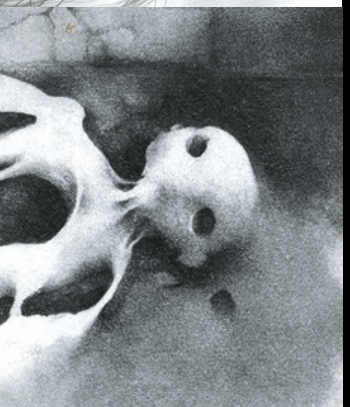
Hybrid UK service?

No UK service?



Weak service for the world?





A Difficult Choice

Large companies may be able to cover these costs, but small companies will suffer

Deja Entendu

Can we save crypto?

accessnow

Furthermore, governments, companies and citizens benefit from maximum security of digital systems. The government endorses the importance of strong encryption for internet security, for supporting the protection of citizens' privacy, for confidential communication by the government and companies, and for the Dutch economy.

accessnow

Amie Stepanovich
amie@accessnow.org

Illustrations: Stephen Gammell,
Scary Stories to Tell in the Dark