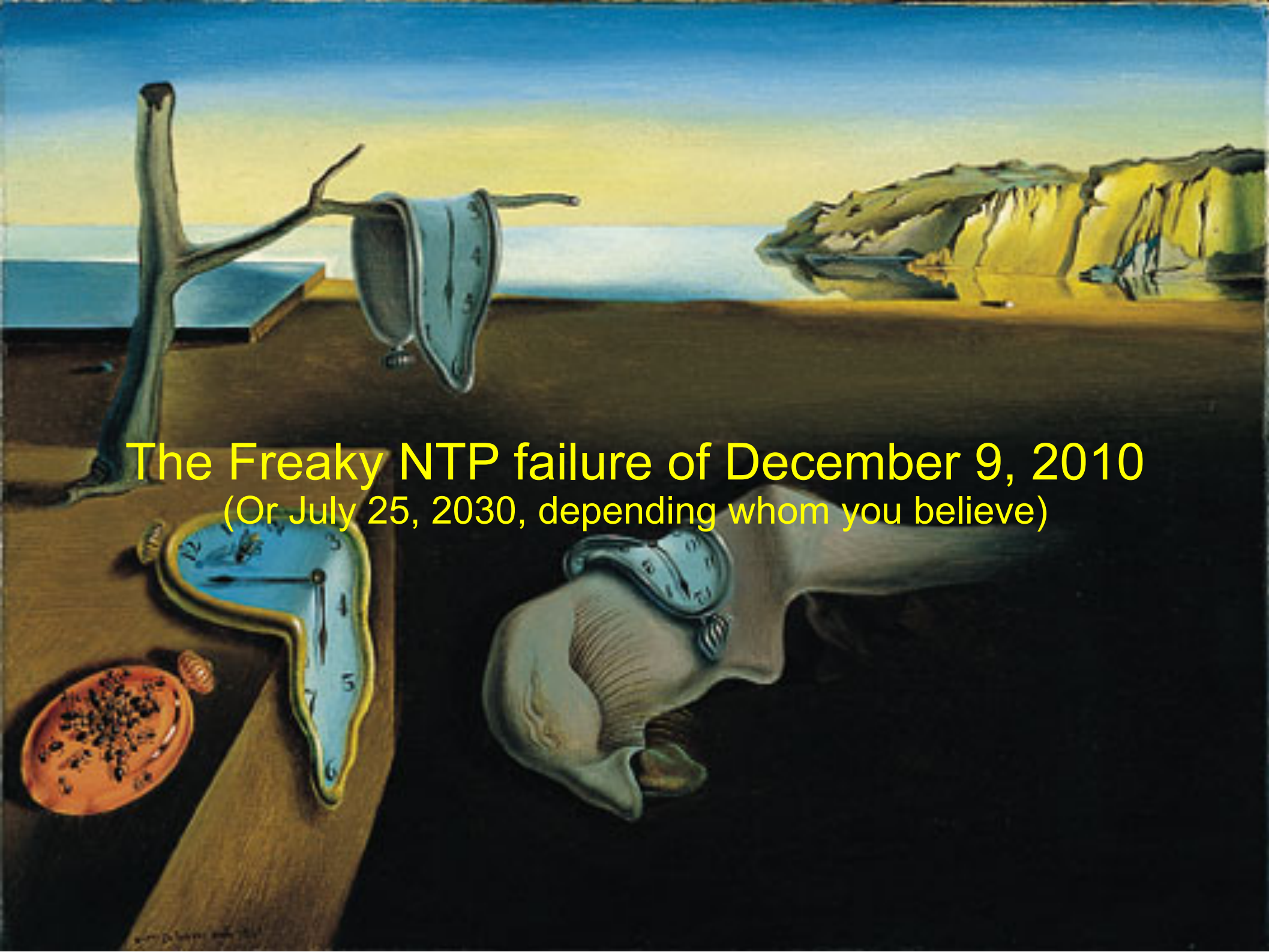
The Freaky NTP failure of December 9, 2010
(Or July 25, 2030, depending whom you believe)

NTP

- Can use multiple sources
- Has sophisticated clock source selection algorithms
- Is pretty finicky about outliers
- Sources report status to assist selection
- Will not accept time input outside certain maximum offsets.
- So, should be relatively resistant to random time inputs, right?

December 9, 2010

- It's 5:45 AM, the phone rings while I'm boarding the bus.
- Our Ops mgr. Is telling me I need to fix the NTP server, which is hosing UH email.
  - What??
- At 2:07 AM, one of our Truetime NTS-200's had decided to report July 25, 2030 as “good” time.

July 25th, 2030

- Of course, no other NTP user or server should be believing this, right?

December 9, 2010

- Nasty old Solaris 8 sez:

Dec 9 03:30:42 ldp11 xntpd447:

ID 261039 daemon.error time error 619315200.095378 is way too large

(set clock manually)

- Great. Good job!

July 25th, 2030

- Much shinier Solaris 10 sez

Dec 9 03:31:12 pub01 xntpd29144: ID 261039 daemon.error time error 619315200.037743 is way too large (set clock manually)

Jul 25 03:31:17 pub01 ntpdate11888: ID 774510 daemon.notice step time server 128.171.3.2 offset 619315200.037684 sec

Jul 25 03:31:17 pub01 xntpd11890: ID 702911 daemon.notice xntpd 3-5.93e+sun 03/08/29 16:23:05 (1.4)

July 25th, 2030

- *ALL* Mac OS X clients said:
  - Duh, OK! July 25th, 2030!
  - Duh....
- No Problems with MS-Windows or Linux came to light.
- Checkpoint firewalls dropped out of HA mode

So the time's wrong, so what?

- All effected systems considered current SSL certificates to be expired 20 years ago
- Email was queued and sent with the wrong date
- SSH Keys were invalidated and then re-generated, so that when the problem was fixed they were re-invalidated, which caused some lockouts.
- Sophos Puremessage declared all email to be dangerous because its virus defs were 20 years out of date.

Playout

- Once I grokked the situation, I called a tech to decapitate the NTP appliance (power plug out)
- Finished my bus ride watching South Park
- Installed the old ANS Surveyor 386 box with a CDMA standard in place of the NTS-200, which is now part of the junk in my office.
- We have one remaining NTS-200 which has shown no signs of malignancy, it needs to be replaced.

Playout

- Googling “July 25, 2030” finds numerous instances of blog and message board posts posted on that date
- We will move to real Linux NTP servers with a “My time is wrong; goodbye cruel world” watchdog script.