



Data Privacy Detective Podcast – Episode 3 – The Battleground of Data and Disclosure

Oct 10, 2016

Categories:

[Blogs](#)

[Podcast](#)

[Publications](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

Eventually, machines were invented to calculate faster and more accurately than humans, and technology replaced human worktime. Computing jobs changed to programmers, website developers and other technicians of today.

In the age of occupational computers, data privacy was virtually non-existent because personal data was sparse. Privacy concerned personal behavior and identity observed directly in person more than through record searches.

Not so today. Personal data is vast and expanding exponentially. And the means of combing through vast quantities of digital data is becoming easier and quicker than ever, with human beings linked to each other on a global scale never before possible. At an October 1, 2016 conference in Luxembourg, French attorney Olivier Saumon cited industry projections that by 2020 the world would have 50 billion connected devices – an average of over five per person. Computers, smartphones, wristwatches, vehicle devices, robots and other devices will create data and connect to an expanding galaxy of devices that will track our health, finances, genetics, emotional make-up, perhaps even our dreams.

France has launched an effort to make medical information more instantly available to approved medical professionals and pharmacies, to look at one example. French citizens may create their own Dossier Médical Personnel, a DMP, which is made available to the creator's medical and pharmacy providers. This can limit accidental allergic reactions or dangerous interactions of prescriptions and improve medical treatment. Over a half million French citizens have created their individual DMP's.

French and European law treats individual health information as highly sensitive personal data. French law provides that health information must be protected from wrongful disclosure and

sharing not expressly consented to by the individual whose data it represents. A French judge recently ordered a website shut down to protect a citizen's DMP. The site was not being handled by an approved host, as it was not linked to a well-established, licensed pharmacy site.

This example shows both how websites are able to search for and secure highly personal health data of individuals and how a government can intervene to delete such information and penalize third parties that lack express consent to handle the information in accordance with French privacy and other regulatory rules. On a deeper level, it highlights the risk associated with efforts to harness technology intended to provide better medical care for individuals who post their data to obtain valuable benefits but then face risks associated with broad sharing of information they assumed would be made available only to approved medical and pharmaceutical providers.

So is technology or the law the issue here? Does one lag behind the other? Experts disagree. But the underlying point is that each of us makes these choices for ourselves – whether to create a medical record for posting and then to review the privacy choices about disclosure before releasing it and limiting it to those with whom we want it shared. Remember, protecting your personal privacy starts with you.

For more information, please contact [Joe Dehner](#) or any attorney in Frost Brown Todd's [Privacy and Information Security Law IndustryGroup](#).

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.