Legal Information Management, 18 (2018), pp. 169–170

doi:10.1017/S1472669618000373

The Tortoise and the Hare? Due Process and Unconstitutionally Obtained Evidence in the Digital Age

Under Moore's Law the number of transistors in an integrated circuit doubles relative to cost and size every two years. In practical terms this means personal computers become twice as powerful and half as large every 24 months. However, this rapid rate of proliferation and improvement has not been mirrored in law.

The law's reaction to digital technologies could be charitably characterised as reflexive. Yoo and Fetzer have remarked that the focus in the early decades of the twenty-first century has remained on the impact of changing social mores, rather than emerging technologies, on legal guarantees.[1] This approach ignores technology's demonstrated tendency to expose latent tensions and force a confrontation with, what Lawrence Tribe might characterize as, the "dark matter" of the law.[2]

These tensions are most obvious in areas where digital technologies have enabled a convergence of surveillance and communication infrastructures - notably in constitutional rights to due process. While the use of algorithms in state decision making, and contractual requirements that remove disputes from public adjudication raise potential due process concerns, the most sustained controversy has been in cases of unconstitutionally obtained evidence.

Under the United States Constitution the 5th and 14th Amendments provide that no person shall be deprived of their life, liberty or property without due process of law. The aspects of procedural due process which flow from these guarantees broadly align with European guarantees under Articles 6 and 7 of the European Convention on Human Rights. Both sets of guarantees guarantee due process (albeit implicitly in the European case) by requiring governments to respect the rights to: an unbiased tribunal, notice, reasons for decisions, an opportunity to respond, cross-examine, examine and offer evidence, receive representation, a public trial and, not be subjected to retrospective prosecution.[3] The ECHR also provides, under Article 13 the right to an effective remedy, a measure not provided in the US.

The US also embraces, as part of due process, those 'fundamental rights implicit in a concept of ordered liberty,'[4] a statement which has been broadly interpreted to import the provisions of the 1st to 8th Amendments within the meaning of due process. In the context of digital technologies, the most important, and controversial, of these has been the 4th Amendment which provides immunity from unreasonable search or seizure of citizens' "persons, houses, papers, and effects" without a warrant based on probable cause.

The tension between emerging technologies and the 4th Amendment is not unique to the digital era. In fact, it began in the 1920s with *Olmstead v United States*,[5] and continued through the twentieth century to the 1967 decision in *Katz*[6] in which the Court established the reasonable expectation of privacy test.

Katz began an ideological trend which still troubles 4th Amendment cases. By promoting a conditioned expectation of privacy the case generated a line of reasoning in which citizens, once informed that they should not expect privacy in respect of a certain area or activity could not exercise a meaningful 4th Amendment claim. The reasonable expectation of privacy test has thus proved suspect. In a modern context, where citizens are aware of large-scale government surveillance in both the US and Europe, a conditioned expectation of privacy does not seem particularly reasonable at all.

The conditioned expectation trend continued in *Smith v Maryland*[7] a decade later, where the Court refused to find that a pen-register (a record of numbers dialled and called) was protected by the 4th Amendment. This rule is known as the third party doctrine and provides that citizens cannot maintain a reasonable expectation of privacy in information voluntarily disclosed to a third party.

The decision in *Smith* was heavily criticised, perhaps most presciently by Justices Marshal and Brennan in their dissent, which condemned the majority for depriving citizens of 4th Amendment protection unless they could forego the use of services which were "a personal and professional necessity."[8] Contemporaneously, the third party doctrine remains the greatest threat to privacy under the 4th Amendment and, by implication, the integrity of due process.

After a period of relative calm, the 4th Amendment found itself before the Court again in 2001 in *Kyllo*.[9] In a decision which indicated that conditioned expectations of privacy were alive and well, the majority ruled that evidence gathered using a thermal imaging device, without a warrant, was unconstitutional. Problematically, the majority based this decision, in part, on the fact the technology employed was not in general public use. The dissent noted as a result that the judgment raised the very real possibility that 4th Amendment protections could diminish rather than increase as more sophisticated surveillance technologies become more publicly accessible.

The importance of the 4th Amendment is evident in light of the convergence of surveillance and communication infrastructures which digital technologies, and third-party involvement in daily communications, have generated. Despite this, limits placed on the 4th Amendment have led many, including Slobogin, to question the relevance of the Amendment in a digital age.[10]

A riposte to such allegations may be imminent. On November 29th 2017 the US Supreme Court heard arguments in *Carpenter v United States*,[11] which asked the court to consider, once again, the third party doctrine, in the context of location data gathered from mobile phones by service providers.

The government contends Carpenter's case is governed by the rule in *Smith* and therefore is not subject to the restrictions of the 4th Amendment.[12] During oral argument, members of the bench questioned whether this was compatible with *Reilly v California*[13] (where a warrant was required under the 4th to search a phone) and *United States v Jones*[14] (where a GPS monitor attached by police to a car fell foul of the 4th Amendment) but Justice Kennedy emphasised the reasonable expectation test, noting he himself expected his phone company tracked his location.[15]

In 2016 Intel announced it no longer follows Moore's Law.[16] Technology may slow, but the law will still struggle to make up ground.

Footnotes

[1] Christopher S Yoo & Thomas Fetzer "New Technologies and Constitutional Law" University of Pennsylvania Law School, Public Law Research Paper no. 13–30.
[2] Lawrence H Tribe "The Invisible Constitution" (Oxford University Press, 2008) p.9.
[3] Judge Henry Friendly has famously enumerated a list of the requirements of Due Process that remains highly influential, see Henry Friendly, 'Some Kind of Hearing' 123 University of Pennsylvania Law Review 1267 (1975).
[4] Palko v. Connecticut, 302 US 319, 325 (1937).
[5] Olmstead v United States 277 US 438.
[6] Katz v United States 389 US 347.
[7] Smith v Maryland 442 US 735.
[8] Ibid., p.751.
[9] Kyllo v United States 533 US 27.
[10] Christopher Slobogin, 'Is the Fourth Amendment Relevant in a Technological Age?' in Jeffrey Rosen and Benjamin Wittes eds "Constitution 3.0: Freedom and Technological Change" (The Brookings Institution, 2011) p.11.
[11] Carpenter v United States 16–402 (2017).
[12] Transcript of Oral argument available at https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/16-402_3f14.pdf (accessed 30/11/17).
[13] Reilly v California 573 US _ (2014).
[14] United States v Jones 565 US 400.
[15] n. 11.
[16] Tom Simonite "Moore's Law is Dead. Now What?" MIT Technology Review at https://www.technologyreview.com/s/601441/moores-law-is-dead-now-what/ (accessed 30/11/17).

Biography

Róisín Costello graduated from the Trinity College School of Law with first class honours and holds Masters degrees in International Affairs and Law from the Institut d'études politiques de Paris and Georgetown Law respectively. During her LLM at Georgetown Róisín was a research assistant for the Georgetown Centre on Privacy and Technology Law and a Consumer Protection and Public Interest clerk at the Electronic Privacy Information Centre in Washington DC. Following graduation Róísín worked in law and policy in London and Dublin including acting as a local expert for the World Bank Report on Women, Business and the Law, and as a policy analyst with the Institute for International and European Affairs. Róisín is currently undertaking her Ph.D. at Trinity College where her research focuses on the impact of digital technologies on fundamental rights and the Rule of Law in the United States and the European Union.

https://doi.org/10.1017/S1472669618000373 Published online by Cambridge University Press