How safe should digital products be, and who should ensure this?

Much of the conversation around the Internet of Things focuses on data protection issues. Here, however, Claire Milne, Visiting Senior Fellow at LSE's Department of Media and Communications, focuses on questions of safety and liability around 'smart' devices.

Widespread recent publicity over Samsung smartphone batteries catching fire has kept ICT product liability in public view. Less visible, but more significant in the long term, is the EU's review of the 1985 Directive on liability for defective products, in the light of "challenges raised by new technological developments, for instance, the Internet of Things or autonomous systems". Plainly, products with a software component open up many new scenarios for malfunction and damage to users, even more so where this software enables communication and action at a distance. Failure of remotely controlled medical devices, or of large moving objects like cars, could have horrible consequences, the latter in particular involving people not party to any relevant agreement.

The EU consultation closed in late April 2017, and at the time of writing, a summary of responses has yet to be published. Meanwhile, we look at some relevant thinking in Europe and elsewhere.

The European consumer representative body BEUC has published its response to the consultation. BEUC stresses that the Directive needs updating not just to encompass digital products, but also in many other respects. It says that the aim of the legislation should be to get the incentives right for preventing consumer damage, as well as ensuring fair compensation when damage does occur. BEUC asserts that "There are no obvious reasons why the liability regime, focusing on the need for compensation of loss or the fair allocation of risks, should not apply to intangible goods such as software or digital content." As well as this extension of the liability regime, BEUC's demands include:

- Extending the scope of liability to include all responsible professionals with a role in complex supply chains.
- Extending the notion of damage to cover non-material damage, for example to the digital environment.
- Rebalancing the burden of proof of damage and its causation from the consumer towards the producer.
- Removing the current 500 euro individual compensation threshold, the 70 million euro aggregate compensation cap, and in suitable cases the ten-year limitation on liability.

Two recent academic papers by lawyers consider such issues more broadly. Alan Butler, Senior Counsel for the US-based Electronic Privacy Information Center (EPIC), has a published preprint titled *Products liability and the internet of (insecure) things: should manufacturers be liable for damage caused by hacked devices?* discussing likely developments in the USA. Butler points out that the large losses associated with cyber-attacks which may be attributed to insecure connected products are likely to give rise to a fresh round of litigation, which will clarify the meaning of existing products liability law in the new context. He argues that Internet of Things (IoT) cases will actually make compensation easier to come by, because the damage caused may be physical as well as economic (whereas isolated software glitches, seen as causing only economic loss, have tended to be undercompensated).

Butler analyses the application to IoT of the "risk-utility defect test", which looks at whether the "foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design", and the "consumer expectations test" which considers whether the product "failed to perform as safely as an ordinary consumer would expect when used in an intended or reasonably foreseeable manner." He thinks that IoT devices would often fail both tests, and also the basic principle that "responsible people should avoid creating opportunities for irresponsible people to do harm." He concludes that a new "post-sale duty to patch vulnerable software" is in order. Indeed, a bill to address this is currently being put forward in California.

In her paper surveying the implications of the new technologies for consumer law in Australia, Kayleen Manwaring, of the University of New South Wales, considers how five distinguishing features of the technologies measure up against basic consumer rights, including the rights to safety and redress which are expressed in products liability law. She concludes, in particular, that the complexity of "eObjects" will lead to uncertainty over how component providers should share liability, and that this will be detrimental not only to consumers, but also more broadly: "Uncertainty as to the extent of legal liability by members of the provider network may well hinder investment and innovation in eObjects".

Clearly, the notion of a safe product can be pushed too far: in principle, design and manufacturing costs could be raised so high that a basically beneficial device can never see light. No doubt this argument will be made forcefully to the EU review by supply side participants. But at present, many observers would say that we are a long way from this danger materialising; on the contrary, the balance needs to move towards protecting consumers, so as to build both safety and well-founded confidence into digital products.

This post gives the views of the author and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics and Political Science.

June 1st, 2017 | Featured, Internet of Things | 1 Comment