The Foundation for Information Policy Research

Consultation response on

Civil Litigation Costs Review

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

FIPR has called for the abolition of the UK's 'loser pays' rule in a number of contexts ranging from privacy to consumer protection[1]. This review is thus of great interest to us. Unfortunately we only learned of it a week before the close of the consultation. We will therefore keep our remarks brief.

1. The transformation of many industries and public services by computers and communications has brought great benefits, but also some harm. FIPR, along with similar NGOs overseas, has been involved in the resulting public policy debates. We have lobbied successfully for amendments to a number of laws that in their original form would have damaged civil rights or consumer protection in the technology context (including the Regulation of Investigatory Powers Act 2000, the Export Control Act 2002, and the EU IP Enforcement Directive). We have also worked to bring together computer scientists, lawyers and economists; one fruit of this has been the new discipline of information security economics[2].
2. But neither legislators nor academic researchers work fast enough to deal with the rapid changes brought about by the Internet. The courts ought to fill this gap. Yet compared with the USA and continental Europe, the UK is falling behind for the simple reason that it is too dangerous for 'normal' people to litigate. No prudent person will sue a bank or government department unless they are wealthy, or

desperate, or somehow shielded from paying costs if they lose.

3. This problem has traditionally been dealt with in the UK by a patchwork of ad-hoc measures: the small claims track in the county court; protective costs orders for judicial review; and specialist bodies such as the Information Commissioner and the Financial Services Ombudsman.
4. However, for various reasons, these provisions are not adequate to deal with many of the new problems being thrown up by technological change.
5. For reasons of brevity, we will discuss only two examples – the arbitration of disputed electronic transactions between banks and their UK customers, and the protection of medical privacy in online systems. These two examples are representative of a very much wider range of problems: a failure of information security is most likely to affect a private citizen or small business either as a financial loss or as a breach of privacy.
6. The rush to take banking services online has resulted, first, in many poorly-designed systems, and second, in banks using their terms and conditions to shift liability for fraud to customers and merchants wherever they can. One example is the EMV 'chip and PIN' system introduced in Europe for debit and credit cards. This has been associated with a 'liability shift' (in the industry's own words[3]) whereby a disputed transaction is charged back to the merchant if no PIN was used, and ascribed to customer negligence or collusion if the bank says that the correct PIN was used. Banks had hoped that this would slash the cost of fraud. However, in the three years since EMV became universal in the UK, banks' card fraud losses have gone up by more than half[4]. (The costs borne by customers and merchants have also gone up sharply, as has the number of disputes.)
7. The reason is simple with hindsight: you cannot expect a system to be secure if one principal guards it, while a different principal pays the costs of failure. The regulators unfortunately ignored the resulting moral hazard.
8. Customers with a payment dispute against their bank are referred to the Financial Ombudsman Service, which provides a dispute resolution service at no cost to the customer (the bank is charged a fixed fee). Indeed the EU Payment Services Directive[5] obliges the UK to provide such a dispute resolution service.

9. However in all cases that have come to our attention, when a customer disputes a card payment, and the bank says that the customer's card and PIN were used, the ombudsman decides in favour of the bank. These decisions frequently fly in the face of both the law and the evidence. We gave two examples in a submission we made to the Hunt Review of the Financial Ombudsman Service, and would respectfully encourage you to read that submission[6]. We believe the evidence presented there will persuade you to question the Consumers' Association view that the ombudsman 'works'. Indeed, the Consumers' Association has published recent research to the effect that 20% of fraud victims end up out of pocket[7].
10. If the regulator has been captured, the next option is the small claims court. Alain Job, an immigrant from the Cameroon, sued the Halifax for some two thousand pounds of disputed ATM transactions, with help from the bar pro bono unit. The bank made the case complex, persuaded the judge to move it from the small claims track to the fast track, prevailed, and got a costs order for £15,000 against Mr Job. Mr Job will not be able to appeal the verdict (on which we take no view here, although it has led to vigorous online discussion[8]). Of relevance here is the fact that fraud victims with even stronger cases than Mr Job, such as Donald and Hazel Reddell whose dispute is described in our submission to the Hunt Review, cannot now risk taking their cases to the small claims court. The protection that court provides against costs orders is quite uncertain.
11. By comparison, in a similar case in Germany, the claimant pursued a bank for €20,000; lost at first instance; and has proceeded to appeal as the costs she had to pay were limited to €2,000. Other countries have seen a variety of outcomes, but with one thing in common: courts can make progress on specific issues.
12. Our second example is medical privacy. The Department of Health is building a number of central data collection systems that privacy campaigners believe to be contrary to law[9].
13. The European Court of Justice decided in I v Finland[10] that patients have the right to restrict their medical records to clinical staff involved directly in their care. Ms I was a nurse in Helsinki who was HIV positive; the systems at the hospital where she worked and was also a patient let all clinical staff see all patients' records; her

colleagues found out about her illness; and they hounded her from her job.

14. Several new central NHS systems hold identifiable personal health data, and while patients may opt out of some of them, this is not allowed for others, notably the NHS Secondary Uses Service (SUS). Privacy campaigners would like to force ministers to allow them to opt out of these others too[11]. We discuss the details in a report, "Database State", that we wrote for the Joseph Rowntree Reform Trust[9].
15. Again, there is a regulator – the Information Commissioner. And yet again, the regulator is ineffective. UK privacy campaigners have often discussed why he is so poor a defender of privacy; our colleagues overseas have had similar discussions. There is a large literature about why regulators are so often captured by the industries they regulate. In the specific case of the Information Commissioner, campaigners complaining of a specific privacy abuse often find that the abusing organisation discussed its proposed use of personal information with officials at the ICO, who did not fully comprehend what was proposed, gave their blessing, and were then unwilling to admit that they could have got it wrong. In a notorious recent case, the ICO (and the Home Office) gave their blessing to unlawful interception by behavioural advertising companies, a decision so egregious that it led the European Commission to take legal action against the UK[12].
16. In any case, the complainant is thrown back on the courts; and once more, campaigners hold back from fear of being bankrupted should they sue and lose. By comparison, privacy campaigners in Germany and the USA can and do bring suit about privacy issues in health, telecoms and elsewhere.

These two examples should illustrate the difficulty faced by citizens in enforcing our rights in the digital age. The loser-pays rule excludes people from justice, and the established exemptions do not adequately cover emerging areas of conflict. One consequence is that human-rights law remains undeveloped in the UK except perhaps in areas that attract legally-aided claimants. Another consequence that we would like to bring to your attention, and that may be of economic importance, is this: the UK is slower at accommodating technological change than countries with better access to justice.

The FIPR position is simple. We advocate a move to the American rule that each side pays its own costs. If there is insufficiently broad support for that, then at the very least, claimants who bring cases founded on the European Convention on Human Rights should be shielded from costs orders, while claimants in other cases should be shielded from costs orders that exceed the amount in dispute, as in Germany. We would not object to the courts being permitted to award costs against anyone whose behaviour has been manifestly unreasonable; however we want an end to the threat of huge costs orders causing manifest injustice.

These were our settled views already; we are grateful to you for providing in your preliminary report so much material, particularly about the detail of costs regimes overseas. From what we have been able to digest, it appears that England may be the worst place in the world for citizens to enforce our digital rights. We hope that your final report will help fix that problem, and are ready to discuss digital policy issues with you in more detail if you feel that would be helpful.

Professor Ross Anderson FRS FREng
Chair, Foundation for Information Policy Research
July 2009

References

[1] See for example 'Consultation Response on the Data Sharing Review', FIPR, Feb 2008, at http://www.fipr.org/080215datasharing.pdf
[2] See the Economics and Security Resource Page, at http://www.cl.cam.ac.uk/~rja14/econsec.html
[3] See for example 'Here comes EMV', *Credit Card Management*, Jan 1 2005, at http://goliath.ecnext.com/coms2/gi_0198-182841/Here-comes-EMV-the-world.html
[4] 'APACS announces latest fraud figures', Oct 1 2008, at http://www.apacs.org.uk/APACSannounceslatestfraudfigures.htm
[5] Directive 2007/64/EC, Nov 13 2007; see in particular articles 80 and 83
[6] 'FIPR Submission to the Hunt Review of the Financial Ombudsman Service', Jan 16 2008; at http://www.fipr.org/080116huntreview.pdf
[7] 'Fraud victims struggle to get money', June 22 2009, at http://www.which.co.uk/news/2009/06/fraud-victims-struggle-to-get-money-back-179150.jsp

[8] 'Chip and PIN on Trial', Light Blue Touchpaper, April 9 2009; at http://www.lightbluetouchpaper.org/2009/04/09/chip-and-pin-on-trial/
[9] See 'Database State', Joseph Rowntree Reform Trust, Mar 2009; at http://www.jrrt.org.uk/uploads/database-state.pdf
[10] I v. Finland, (2009) 48 EHRR 31, [2008] ECHR 623, at http://www.bailii.org/eu/cases/ECHR/2008/623.html
[11] For detailed background see discussion in reference [1] above
[12] See 'EC Starts legal Action over Phorm', BBC, April 14 2009, at http://news.bbc.co.uk/1/hi/technology/7998009.stm; 'Open Letter to the Information Commissioner', Mar 7 2008, at http://www.fipr.org/080317icoletter.html; 'Profiling web users – some intellectual property problems', Computers and Law Nov 2008, at http://www.fipr.org/0811SCLarticle.pdf; and 'Further Legal Problems for Phorm' at http://www.fipr.org/press/081125phorm.html