newlawjournal.co.uk VOL 165 7642 | £8.00 27 February 2015

New Law Journal

Leading on debate, litigation and dispute resolution

Happy anniversary?
A year of sweeping family law reform

Survival of the fittest
Patrick Allen counts the cost of the Jackson reforms & legal aid cuts

The inexpert expert
A checklist for solicitors instructing experts who are courtroom novices

Big Brother

A step too far?

ISSN 0306-6479

Commercial: clarity for credit agreement claims

Access all areas?

Overriding lawyer-client & confidential communications is incompatible with the rule of law, as Nicholas Griffin QC, Robert O'Sullivan QC & Gordon Nardell QC explain

IN BRIEF

- Legal professional privilege is of fundamental importance to the administration of justice. It must be afforded greater protection from state surveillance activities, even in a time of heightened concerns about terrorist activity.
- Confidential journalists' communications must also be protected. Existing legislative safeguards must not be bypassed by the state and additional protections must be built into the system.

On 11 January the prime minister attended the unity march in Paris following the murders of 17 journalists, shoppers and police officers in that city by terrorists. He was there in a demonstration of solidarity with the French, condemning the attacks as unacceptable in a free, open and tolerant country. And yet at the same time he was advocating ever greater powers for the police and the security agencies to intrude on our private communications. Deputy Prime Minister Nick Clegg noted the irony, commenting on politicians: "who say in one breath that they will defend freedom of expression and then in the next advocate a huge encroachment on the freedom of all British citizens".

This is the difficult atmosphere in which decisions must be made about the proper extent of powers for the state to access our communications. In this article we focus primarily on the protection to be given to lawyer-client communications and to other categories of confidential information, most particularly between journalists and their sources.

Principle

Legal professional privilege (LPP) is a principle of law which the late Lord Chief Justice Lord Taylor described as "a fundamental condition on which the administration of justice as a whole rests" (*R v Derby Magistrates' Court ex parte B* [1996] AC 487, [1995] 4 All ER 526). As every judge, practitioner and law student knows, it entitles a person to consult with his lawyer confident that the communication, whether in person, by letter, telephone call, or electronic means will forever remain private. It is a privilege held by the client, not the lawyer, and can only be waived by the client. In principle it is an absolute privilege (see below) subject only to the rule that it does not protect communications in furtherance of crime: the "iniquity exception". Every individual who has cause to seek legal advice, whether in the context of litigation or not, must do so in the sure knowledge that what he says and what he is told will not be revealed and used to his detriment. Without LPP, the full truth will not be told and advice will be given on a false premise. The privilege is never more necessary than when an individual is in criminal or civil litigation with the state, with its wide-ranging powers of covert surveillance.

Confidence

The right of individuals to communicate in confidence about personal or sensitive information is not limited to the lawyers and their clients. Journalists play a crucial role in exposing abuse of power in the public and private sectors, and in revealing and remedying miscarriages of justice. In January 2015 the editors of every national newspaper published an open letter in the *Press Gazette* emphasising the public interest in whistleblowers speaking to journalists confident in the protection of their identity. Part 2 of the Police and Criminal Evidence Act 1984 (PACE 1984) already protects personal records and journalistic material held in confidence from seizure without a warrant issued by a judge.

Securing citizens' safety v respecting privacy

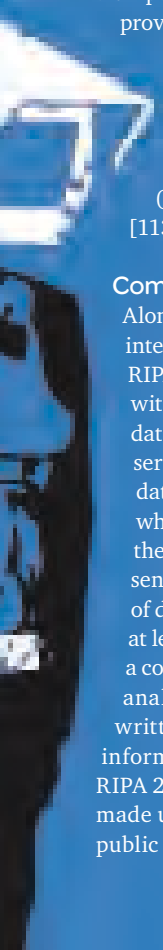
Amid the propaganda on all sides, it is hard to say how far the British public is genuinely prepared to surrender certain rights and freedoms to achieve increased safety at a time of heightened threat. It is difficult in principle to calculate just how much privacy we should surrender for better safety and vice versa because we are not dealing with commensurate values. But we suggest that Parliament has failed to achieve the correct balance in its legislation in the new Millennium—and is in danger of falling into even deeper error. It is a situation that Parliament must address.

Surveillance, CHIS, interception

The state has at its disposal a formidable arsenal of covert surveillance powers, which are principally to be found in the Regulation of Investigative Powers Act 2000 (RIPA 2000) and five associated Codes of Practice. Part 1 of RIPA 2000 enables prescribed public authorities (which include the Metropolitan Police, the Security and Secret Intelligence Services, the National Crime Agency and HM Revenue and Customs) on the authorisation of a warrant issued by the home secretary, to intercept communications. Part 2 empowers public authorities (which additionally include police forces, the Serious Fraud Office, the armed forces, various government departments and local county or district councils) covertly to monitor, listen, observe and record the movements and communications of others. That surveillance can be undertaken in person by a covert human intelligence source (CHIS), or remotely through electronic devices placed in a private residence or vehicle (intrusive surveillance) or by observation in public or on premises such as offices, prisons and police stations (directed surveillance). Part 2 surveillance is

subject to an authorisation being issued by a specified senior officer in the authority which conducts the surveillance. There is no direct judicial oversight of any covert surveillance under Pt 2.

In contrast to police powers under PACE 1984, none of RIPA 2000's information-gathering powers is expressed to be subject to LPP; the privilege is not mentioned in the Act. The recently re-amended and draft amended Codes of Practice do acknowledge the existence of LLP but approve the intentional breach of the privilege in certain "exceptional and compelling circumstances"—though on closer examination the circumstances may not in fact be that "exceptional" in practice; according to the Codes, they are not restricted to the situation where national security is threatened but may also arise where there is a "threat to life or limb", which potentially covers a great deal of ground. The Codes simply refer to "similar consideration" being given to journalistic information and confidential personal information. In respect of LPP, and to the surprise of many practitioners, the Codes accurately reflect the current state of the law. The House of Lords in *McE v Prison Service of Northern Ireland* [2009] 1 AC 908, [2009] 2 WLR 782 (notably, Lord Phillips dissenting) held that Pt 2 of RIPA 2000 permitted the covert surveillance of a meeting between a lawyer and his client (a remand prisoner). RIPA 2000 effectively trumped s 58 of PACE 1984, which expressly provides that such a communication shall be "private", notwithstanding that the surveillance breached the appellant's rights under Art 8(1) of the European Convention on Human Rights (the Convention) (judgment paras [75], [95] and [113]).



Communications data

Alongside the provisions about interception of communications, Pt 1 of RIPA 2000 provides public authorities with power to acquire communications data held by postal, telephone and digital service providers. Communications data consists of the "who, what, when, where" of a communication: the identity and whereabouts of the sender and recipient, the date and time of dispatch and delivery. Historically at least, it differs from the content of a communication; an often-quoted analogy is with the information written on an envelope (data) and the information in the letter inside (content). RIPA 2000 and a succession of orders made under it empower a wide range of public bodies to access communications data. Like the Pt 2 surveillance powers, there is no requirement for a warrant; with the exception of local authorities, bodies can grant themselves authorisation via a senior officer.

Service providers would not ordinarily retain data about communications they carry for longer than needed for business purposes. But in 2006 the EU, prompted by the UK, adopted the Data Retention Directive 2006/24/EC, obliging member states to require providers to retain records for between six months and two years. This created the pool of data from which RIPA acquisition requests could be made. With the growth of phenomena such as cloud computing and social media, the distinction between "content" and "data" has gradually eroded. Information about who contacted whom, how, when, where, and about what, enables the authorities to paint a vivid picture of a person's contacts, activities and interests. So "blanket" data retention—requiring everyone's data to be kept, regardless of whether they are under suspicion, just in case it might later be of interest—has given rise to growing privacy concerns. On 8 April 2014, the Court of Justice of the European Union (CJEU) in joined cases *Digital Rights Ireland Ltd* and *Kärntner Landesregierung C-293/12 and C-594/12*, [2014] 2 All ER (Comm) 1 gave judgment annulling the Directive, finding that it created a "particularly serious interference" with rights under Arts 7 and 8 of the EU Charter of Fundamental Rights (corresponding to Art 8 of the Convention). The UK government responded by fast-tracking through Parliament the Data Retention and Investigatory Powers Act 2014 (DRIPA 2014), which broadly replicated the Data Retention Directive regime. DRIPA 2014 is now under a human rights and EU law challenge in judicial review proceedings on much the same grounds as led the CJEU to strike down the Directive.

How should RIPA deal with LPP?

McE was met with alarm by the Bar. The RIPA 2000 provisions about interception, CHIS and communications data are framed in similar terms to the directed surveillance provisions, so the decision also disapplies the protection of LPP from those techniques (see ss 1(5), 21(2) and 27(1)). Allowing investigating authorities to use their panoply of covert powers deliberately to monitor privileged lawyer-client communications is in obvious conflict with the rationale of LPP and poses a significant risk to the fairness of subsequent proceedings. That risk materialised in the wake of revelations about the infiltration of campaign groups by undercover police officers including PC Mark Kennedy. Groups of protesters are likely to obtain advice en masse where criminal proceedings have been brought against members, and there are obvious problems of fair trial where a serving police officer makes himself privy to such information. In *Barkshire & Others v R* [2011] EWCA Crim 1885, [2011] All ER (D) 180 (Jul), Kennedy's activities led to successful appeals by 20 individuals against their convictions. The Court of Appeal expressed disquiet at the possibility that privileged communications may have found their way to Kennedy's handlers or the prosecution. More recently, it emerged in the *Belhaj* litigation in the Investigatory Powers Tribunal that internal guidance within the security and intelligence agencies had conflicted with the RIPA 2000 Codes, undermining even the limited protection the Codes offer.

Wherever precisely the balance between privacy and security ought to lie, empowering the authorities secretly to override LPP is simply incompatible with the rule of law. Particularly disturbing is the House of Lords' conclusion in *McE* that Parliament must be taken as having decided, by implication and without any debate, to dispense with this cornerstone of justice. In an attempt to resolve the issue, the Bar Council sponsored amendments to the Bill for the Protection of Freedoms Act 2012. Moved in the Lords by Baroness Sally Hamwee, these would have brought RIPA 2000 into line with PACE 1984 by preventing the authorities from targeting privileged communications while preserving the iniquity exception. The government opposed the change, insisting that nobody could be "above the law" and suggesting that the lawyer-client relationship could be abused for terrorist purposes. The government won the day, but lost the argument. The Minister, Lord Henley, could give no example of a situation in which the iniquity exception would not cover terrorist misuse of lawyer-client communications.

LPP concerns apply in a slightly different way to communications data. The RIPA Codes on communications data, like their counterparts for interception, surveillance and CHIS, contemplate that the authorities may target information relating to lawyer-client communications. Because (in theory at least) the data does not reveal the content of communications, retaining or accessing that data is not considered to involve a breach of privilege. However, as noted, in reality communications data can impart much information about the context and purpose of a communication, enabling the authorities to draw potentially reliable inferences about what may have been

discussed, who else is involved, and so on. The availability of that information to an investigating or prosecuting authority raises an obvious inequality of arms and risks miscarriages of justice. Also now clear is the potential for abuse of RIPA 2000 communications data powers. The *Press Gazette* letter was prompted by revelations in 2014 that the police had routinely made RIPA 2000 requests to access journalists' mobile phone records, sidestepping the restrictions and safeguards PACE 1984 provides for journalistic material.

All this adds up to an irresistible case for amending RIPA 2000 so that LPP and other vital relationships of confidence are properly protected by primary legislation following thorough consideration in Parliament.

Future trends

The sunset clause in DRIPA 2014 will require the new government to legislate again before the end of 2016—and will provide an opportunity for fundamental review of the statutory framework in which public authorities now operate. The new legislation will be informed by a review of communications data and interception powers currently being conducted by David Anderson QC, the Independent Reviewer of Terrorism Legislation, by a review into surveillance powers conducted by the Royal United Services Institute, and by the Intelligence and Security Committee's Inquiry into Privacy and Security.

Both past and present governments have in recent years pressed for increased surveillance powers. The current government's draft Communications Data Bill (2012)—the "snoopers' charter"—required retention of new categories of communications data, identified by Home Office officials as including:

- data showing who is using an IP address at any given point;
- data identifying which services or websites are used on the internet; and
- data from providers based overseas who provide webmail and social networks to users in the UK.

The Bill was heavily criticised, among other things for eroding the distinction between content and data. It was dropped when the Liberal Democrats refused to support it.

However, the Counter-Terrorism and Security Act 2015 received Royal Assent on 12 February and contains a raft of new measures. Among them is, once again, the power to identify who is using an IP address (Pt 3, yet to come into force).

It is clear from recent pronouncements, during and following the Paris attacks, that a new Conservative government would seek to bring back a beefed-up Communications Data Bill, with new powers in areas such as encrypted communications.

Labour believe the Communications Data Bill is too widely drawn and have called for a full review of RIPA 2000 itself. However, it is unclear at present what a new Labour government would actually do in power. Some indication of future approach may be discerned from its support last year for DRIPA 2014.

What happens now?

In the present febrile atmosphere it is more important than ever that voices within and beyond the legal profession speak up for LPP. The Bar Council continues to press the case for amendments to RIPA 2000. The Chairman of the Bar has written to the independent reviewer of terrorism legislation, David Anderson QC, inviting him to support the case for reform of the law as part of his ongoing Investigatory Powers Review, due to report in spring. While the RIPA 2000 Codes of Practice must inevitably reflect the present state of the law, they can and should be amended in the meantime to reduce to a bare minimum the scope for deliberate monitoring of lawyer-client communications and to introduce additional safeguards for this dangerous practice. The Home Office recently consulted on new draft Codes for communications data. The Bar Council was among those who responded, suggesting changes to deal not only with LPP but the problem of improper accessing of journalists' call records. The journalistic community is also arguing for reform. A coalition for long-overdue change is taking shape.

There is some cause for hope—at least for the journalists. Following recommendations made in February by the Interception Commissioner, the government has just agreed to introduce interim guidelines requiring the police to use judicially authorised PACE production orders (as opposed to RIPA authorisations) to get hold of communications data revealing journalistic sources. We are yet to see the detail. The government, if re-elected, has said it would introduce legislation to achieve the same purpose.

Comment

The battle for proper protection for privileged and confidential information is currently being fought. New legislation early in the new Parliament (and the scrutiny and reconsideration of underlying principles that must inevitably accompany it) should provide lawyers as well as journalists with a renewed opportunity to make—and win—our arguments. **NLJ**

Nicholas Griffin QC & **Robert O'Sullivan QC** are members of 5 Paper Buildings (*www.5pb.co.uk*) & **Gordon Nardell QC** is a member of 39 Essex Chambers (*www.39essex.com*). All are members of the Bar Council's Law Reform Committee and Working Group on Surveillance and Privacy, although this article is written in a personal capacity.