e-commercelawreports

THE PRACTITIONERS' GUIDE TO E-COMMERCE CASES
VOLUME 13 ISSUE 06 **WWW.E-COMLAW.COM**
[2013] ECLR 1- 24

VOLUME 13 ISSUE 06 **[2013] ECLR 1-24**

e-commercelawreports
THE PRACTITIONERS' GUIDE TO E-COMMERCE CASES
[2013] ECLR 1-24 VOLUME 13 ISSUE 06
WWW.E-COMLAW.COM

EDITORIAL

Editorial: SAS v. WPL

The UK Court of Appeal ruled on 21 November in the dispute between SAS Institute Inc. and World Programming Ltd. (WPL) that the functionality and programming of a computer program is not protected by copyright, finding, as the English High Court did, in WPL's favour.

The litigation began when WPL developed a software system that was functionally equivalent to components of programs developed by SAS. Both systems allow users to write applications; SAS' system requires that this is done in SAS programming language while WPL's system allows the use of other programming languages such as C++. WPL, which had a customer licence from SAS, was aided by a 'Learning Edition' provided by SAS – designed for customers' use in understanding SAS products – and a SAS user manual; both were utilised by WPL alongside the SAS system to observe and test how the SAS programs worked and to thus aid in WPL's own design.

SAS litigated against WPL on a number of copyright claims both in terms of the system and the manual. These included the claim that WPL, in producing a system heavily based on the functionality of SAS' program, infringed SAS' system copyright.

Following a judgment in the English High Court by Arnold J and a referral to the CJEU, before Arnold J maintained his position in a second instance judgment, SAS brought the matter to the attention of Lewison LJ in the Court of Appeal. Lewison LJ found that software functionality could not be protected by copyright since functionality does not represent the expression of an intellectual creation. Instead, such expression remains with the source code for the program, which WPL had not been privy to. WPL's functional recreation of SAS' system instead was born from studying the program, as well as the literature SAS provided to its customers. Had WPL been able to access the source code and then copied it, this would have been an infringement of copyright.

The Court ruled that insofar as the ideas in the user manual were concerned, the manual described through its keywords, formulae and so on the functionality of the system it was produced to aid with – and the system's functionality was not an expression of an intellectual creation.

Those involved in software will need to consider the consequences of this decision. For a start, the extent to which copyright can be found in a program is clearer than ever before. This will present opportunities for developers provided that they merely study and test a program's functionality as WPL did here. Meanwhile, developers will want to avoid finding themselves in a position akin to that of SAS. Will functionally very similar programs become more common? If so, given that the challenge of proving infringement of copyright in a software system is now a more difficult one without a provable infringement of a source code, developers may find themselves in a more competitive market.

CECILE PARK PUBLISHING
Managing Editor Lindsey Greig
lindsey.greig@e-comlaw.com
Editor Sophie Cameron
sophie.cameron@e-comlaw.com
Associate Editor Simon Fuller
simon.fuller@e-comlaw.com
Subscriptions Adelaide Pearce
adelaide.pearce@e-comlaw.com
telephone +44 (0)20 7012 1387
Design MadeInEarnest
www.madeinearnest.com

E-Commerce Law Reports is published by Cecile Park Publishing Limited
17 The Timber Yard, Drysdale Street, London N1 6ND
telephone +44 (0)20 7012 1380
facsimile +44 (0)20 7729 6093
www.e-comlaw.com

Google and the digital privacy perfect storm

In three unrelated class actions, Google Inc. is defending wiretap claims related to web tracking, email scanning, and Wi-Fi sniffing. These lawsuits will define digital privacy rights for at least a generation and will test Silicon Valley's guiding spirit.

Background

An evaluation of Google's situation requires an understanding of a number of fundamental and conflicting forces.

1. Advertising is king

When something online is free, you're not the customer, you're the product. In other words, free content brings viewers, and the advertisers pay for the content. As a business model, this bargain is nothing new, but the interactive nature of the internet changes the model. For the first time, content providers have the technological ability to move beyond simply delivering content to the user, and can now collect data on the user - and then correlate, repackage and sell the data.

Many email services are also now free to the user because the webmail interface is a platform to deliver advertising. Social media complicates the picture exponentially because viewing habits can be correlated with sensitive personal information often volunteered by the user. Add to this a network effect producing massive aggregations of data, tumbling e-storage costs, and a new imperative to increase revenues following several recent IPOs, and it becomes nearly impossible for internet companies to resist pressures to push the envelope in efforts to gather ever-detailed personal data.

2. Diverging views of privacy

The second force shaping the digital privacy debate is the sharp divergence in views between industry and the general public. A handful of technology companies now control personal data on almost half the world's population. Google's stated mission is 'to organize the world's information' - an idea once seemingly daft but now eminently believable.

In contrast the public increasingly values privacy. The tipping point in this standoff follows the revelations of surveillance conducted by the US National Security Agency. Although NSA surveillance raises issues of government conduct, it has awoken the public to the issue of surveillance more broadly.

Digital privacy is one of the few issues that cuts across the political spectrum. Internet privacy is now identified by the American Civil Liberties Union ('ACLU') as a 'key issue' - and because government surveillance is now largely built on private surveillance, the ACLU takes the position that e-commerce companies must be the 'first line of defense when it comes to keeping private information private.' The ACLU is taking the lead in court battles over NSA surveillance. On the other end of the spectrum, libertarians and conservatives are quick to note the link between privacy and ordered liberty: 'Civilization is the progress toward a society of privacy.'[1] In this regard, a conservative might agree with Google's Vint Cerf's comments at a recent FTC forum that "it's the industrial revolution and the growth of urban concentrations that led to a sense of anonymity" but would disagree with his belief that such anonymity is a mere historical aberration.

3. Contract-based regulation

The third force shaping the debate is the complex mechanism for protecting privacy in the US. The word 'privacy' appears nowhere in the Constitution. Although the Fourth Amendment preserves the right to be free from search or seizure without a warrant, the right is trespass-based; privacy as its own right came later. In 1853, Francis Lieber, advisor to President Lincoln, wrote 'No one can imagine himself free if his communion with his fellows is interrupted or submitted to surveillance.'[2] In 1890, two young lawyers, Samuel Warren and Louis Brandeis argued for a common-law right of privacy in an influential Harvard Law Review - no state recognised such a right in 1890.

In the Olmstead case of 1928, the US Supreme Court refused to extend the Fourth Amendment to wiretaps, on the theory that there was no trespass[3]. But the case is more famous for the dissent of Justice Brandeis, who predicted the rise of electronic surveillance: 'Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . Can it be that the Constitution affords no protection against such invasions of individual security?'

Forty years later, Justice Brandeis' dissent was adopted by the Court in the landmark Katz decision[4]. Constitutional notions of privacy were now de-linked from 'trespass' and defined by the public's 'reasonable expectations of privacy.' Congress responded by passing the Omnibus Crime Control and Safe Streets Act[5], otherwise known as the 'Wiretap Law,' which promulgated rules governing the interception of telephone communications. In 1986, the Wiretap Law was amended by the Electronic Communications Privacy Act of 1986 ('ECPA') to include a broader range of communications. Title I of the ECPA includes an amended Wiretap Act, and Title II provides a new Stored Communications Act ('SCA') providing protections to communications in temporary storage. Congress also passed the Computer Fraud and Abuse Act ('CFAA').

The original Wiretap Law and the

ECPA amendments were meant to accommodate the Katz court's 'reasonable expectations of privacy,' but the laws went further - Congress explicitly adopted a consent-based regime. Thus, if no party to a telephone or email communication consents to the interception of voice or data, federal law forbids the interception without a warrant or other similar protections.

In 1993, the internet went mainstream. Immediately recognising its transformative potential, the Clinton White House promulgated principles to govern its future growth and regulation in 'A Framework for Global Economic Commerce,' or the 'Clinton-Gore Framework.' The Clinton-Gore Framework extends the consent-based model of the ECPA, and adopts a free-market and self-regulation approach to e-commerce, including contract-based privacy rights. Although the Framework is not a law *per se*, its logic has been implicitly adopted by courts ever since. Thus, the ECPA's prohibitions against interceptions of electronic data depend on the interception being non-consensual even in the internet age; if one party contractually consents to the intercept, it is lawful.

Web-tracking

As originally conceived by Sir Tim Berners-Lee (the inventor of the web) cookies were meant to facilitate the conversation between the user and the website, nothing more. However, websites offering 'free' content quickly realised that they could contract with third-party 'ad serving' companies to write persistent cookies that, when synchronised with other cookies, allowed for the tracking of each web users' internet usage and other sensitive personal information. In exchange for allowing this tracking, the website would receive money. The third party would build a digital dossier on the user with detailed personal information gleaned from the tracking. That information could then be used to target advertising to the user.

One of the first internet ad-serving companies was DoubleClick, founded in 1995. Because DoubleClick's third-party tracking cookies essentially enabled the interception of users' communications with external websites, a consumer class action was filed in New York in 2000 alleging that the tracking violated the SCA, the Wiretap Act and the CFAA, along with various common law rights. In what is largely considered the most important internet privacy judicial opinion ever written, Judge Buchwald dismissed the case largely on the theory of consent. Because browsers can be set to block third-party cookies, a user consents to the tracking if the blocking feature is not enabled[6]. Judge Buchwald's opinion thus implicitly adopted the Clinton-Gore Framework. If a user consents to the interception, it cannot violate any contract-based privacy laws.

But what happens if a user does not consent, and is tracked anyway? Three class actions are exploring this very question[7].

1. Google, Inc. cookie placement consumer privacy litigation (2013 WL 5582866 (9 Oct 2013)).

This class action followed revelations in 2012 that Google's DoubleClick subsidiary and three online advertising companies were circumventing the privacy settings of Apple's Safari browser. In 2004, Apple decided to enable cookie-blocking protection by default, and marketed the product as better protected against unwanted tracking. Starting in 2010, however, several companies found a way to hack Safari to trick the browser into accepting third-party cookies. Google admitted to the hacking, but argued that it had merely 'used known Safari functionality.'

The Federal Trade Commission ('FTC') charged that Google's actions violated a previous settlement and violated its own privacy policy, and fined the company $22.5 million. Although the fine was a record for this type of violation, the enforcement action was largely derided as laughably small. The fine represented less than four hours of revenues for the company and no effort was made to quantify the excess revenues attributable to the violation. None of the fine was distributed to Safari users whose data was taken without permission. Later, 37 states found that Google's actions violated various state consumer protection laws, and fined the company $17 million.

Safari users filed their own private suits consolidated in Delaware before Judge Robinson. The plaintiffs asserted claims under the ECPA and various California laws. Judge Robinson found Google's actions 'objectionable' and ruled that Google was not an authorised party to the intercepted communications because it did not have consent to circumvent the privacy settings of the browsers. Nevertheless, she dismissed the case in its entirety. It was a near-complete victory for Google, but the decision is on appeal to the Third Circuit Court of Appeals[8].

The Google 'Safari-Hacking' appeal will address five questions with far-reaching implications. Two of these questions stand out. First, does web tracking involve the interception of 'content' when URLs are tracked? If these URLs are deemed not to contain 'content,' there is no violation under the Wiretap Act nor the

SCA, both of which only prohibit the interception of content. Because URLs can include search terms and other substantive information, they betray far greater information than IP addresses. Judge Robinson held that URLs do not contain content, even if tracking may involve the interception of 'communications.'

Second, are consumers harmed when they are tracked and their personally identifiable information is taken without their consent? Because the Wiretap Act and SCA only provide statutory damages when 'content' is intercepted, many consumers turn to state consumer protection laws and common law remedies. But some state statutes require actual out-of-pocket losses in order for the claim to be cognisable, and Judge Robinson found that the mere theft of personal information - even without consent, and even via hacking - is not sufficient 'harm' under the Constitution to assert any common law claims. Although Judge Robinson's view of 'harm' is supported by other judges, there is other authority that runs counter. The FTC recently charged rent-to-own company Aaron's, Inc. with violations of federal law by secretly installing tracking software on rented laptops without consumer consent. The software tracked sensitive personal information but no consumer suffered any out-of-pocket damages. Nevertheless, the FTC took the position that the unwanted tracking of personal information was harm in and of itself and prosecuted Aaron's.

Interestingly, Google chose not to cross-appeal the one issue it lost. Crucially, the court found lack of consent to the tracking even though the protection was a default setting not affirmatively set by the user. Now that Google has chosen not to appeal this portion of the ruling, what impact does it have?

This question will have vastly increased importance after 1 January 2014 when web companies doing business in California are required to disclose whether they respect Do Not Track ('DNT') signals. DNT signals are HTTP header fields sent by a user's browser that tell external websites not to track the user. Does a DNT signal negate consent when the browser clearly tells websites that the user does not want to be tracked? Does it matter if the DNT signal is a default setting, or affirmatively chosen by the user? Under Judge Robinson's Google holding, the answer seems to be an unequivocal no to both questions - the third party is not an authorised party to the communication. If the Third Circuit overturns Judge Robinson's 'content' holding, Google's acquiescence on the 'consent' holding will have enormous consequences for DNT and future web tracking liability.

2. Other web tracking cases

There are three other cases currently asking the same questions. In re: Facebook Internet Tracking Litigation, pending in the Northern District of California[9], Facebook was caught tracking members' internet use beyond the scope of consent. Facebook agreed to stop tracking members post-logout after the practice was disclosed by the press, and users filed claims under Titles I and II of the ECPA, the CFAA and various California state laws. An unrelated case in New Jersey against Viacom (and Google) is also testing many of the same issues, except that the case is brought on behalf of minors[10]. Finally, the most recent of the web tracking cases is Mount v. PulsePoint, Inc., pending in New York. PulsePoint was caught hacking Safari's privacy protections, paid a fine, and agreed to stop the practice. The issues echo the Google case, except that New York claims are asserted instead of California claims[11]. Importantly, the PulsePoint case has been assigned to Judge Buchwald, the author of the DoubleClick opinion[12].

Email-scanning

The second test of America's digital privacy paradigm is the Google Inc. Gmail Litigation pending in the N. D. Cal[13]. Originally a much smaller case brought on behalf of email users in Texas, it eventually merged with other cases and grew into a multi-billion-dollar headache for Google. Gmail is a 'free' email service, and Google makes money by delivering advertising to users. In 2004, Google announced that it would start scanning emails for content to enable the company to serve tailored ads and charge more to advertisers. Although some privacy advocates such as the Electronic Privacy Information Center objected and asked the California Attorney General's office to investigate, Google won the day with its argument that it obtained user consent in the Terms of Use.

However, not all users believed they consented to the scanning. Other cases were soon filed, and the cases were consolidated in California. In a landmark opinion a federal court held that the gmail Terms of Use were insufficient to obtain valid consent from any gmail subscriber - and no attempt was made to obtain consent from non-subscribers who emailed subscribers[14]. The court held that the Terms of Use must be explicit and understandable, and must state the purpose of the scanning. Google informed gmail users that emails might be scanned for content, but the Terms of Use did not say it would be scanned, did not disclose the purpose or that

user profiles would be created. Google has requested permission for interlocutory appeal, and the request is under consideration.

The 'gmail' case will have implications far beyond Google. In a consent-based system involving e-commerce, contracts are often formed by users clicking 'yes' in a box following or preceding the phrase 'I accept the Terms of Use.' When users visit websites as visitors and not registered users, the website simply notes in small print that use of the website is conditioned on acceptance of a Terms of Use, and consent is assumed even without the affirmative action. Almost no one ever reads the terms of use governing the privacy policies of websites, including the Chief Justice of the US Supreme Court, raising the question of their enforceability and the viability of the Clinton-Gore Framework.

And the difficulty extends beyond wiretapping. Some companies are burying non-disparagement clauses in their Terms of Use that no reasonable consumer would ever read or accept. KlearGear included a clause in the Terms of Use penalising consumers $3,500 for making negative comments about the company; when one customer posted a negative review following the failure to deliver a product, the customer was sued. Although not a wiretap case, the question of whether a valid contract was formed mirrors the 'consent' issue in the gmail case.

Wi-Fi sniffing

The third wiretap case involving Google is the Street View case[15], a fascinating illustration of the difficulty applying outdated statutes to new technology. In 2007, Google launched its 'street view' feature. Between 2007 and 2010, while photograhing the public from public streets, Google surreptitiously captured data leaking from unencrypted Wi-Fi networks. Such data included personal emails, usernames, and passwords. As with other privacy violations, Google agreed to stop the practice after it was caught, and was fined $25,000 by the FTC and €145,000 by the German privacy regulator. Consumers also sued under the Wiretap Act and various California laws, arguing that confidential communications were intercepted without consent. There is no doubt that the payload data are 'communications' within the meaning of the Wiretap Act, and there is no doubt that the users of the unencrypted Wi-Fi networks never explicitly gave Google consent to gathering the data. However, Google argued that the law did not apply - the communications could not be 'private' if unencrypted and leaking beyond the property lines, and there is a statutory exception for radio communications readily accessible to the public.

A federal court in California rejected Google's defences. Because the Wiretap Act provides $100 statutory damages to each person whose communications were intercepted, Google could face more than $1 billion in damages. The exposure increased when a three-judge panel of the Ninth Circuit Court of Appeals affirmed the lower court's decision to reject the 'readily accessible' defence[16]. Google has requested *en banc* review, which is pending. Google's mission will depend on a statutory reading of an exception to the prohibition against intercepting electronic communications. The only way Google can prevail is if a group of judges interpret the term 'radio' to encompass a technology that did not exist when the ECPA was enacted.

Conclusion

The push for ever-larger online advertising revenues requires ever-increasing surveillance of internet users, while at the same time the public is becoming uncomfortable with the concomitant loss of privacy rights. Add to that dynamic a largely contract-based regime built on 'consent,' a government enforcement effort largely viewed as impotent, and a judiciary increasingly open to privacy-related class actions, and a perfect legal storm has formed that will define digital privacy rights in the US for the next generation. And Google is at the centre.

David Straite Of Counsel
Laurence King Partner
Kaplan Fox & Kilsheimer LLP
DStraite@kaplanfox.com
LKing@kaplanfox.com

A longer version of this article is featured online. *David and Larry represent consumers in digital privacy cases.*

1. Ayn Rand, The Fountainhead at p. 715 (1943).
2. Francis Lieber, On Civil Liberty and Self-Government, ch. IX (1853).
3. Olmstead v. United States, 277 U.S. 438 (1928).
4. Katz v. United States, 389 U.S. 347 (1967).
5. Codified at 42 USC 3711.
6. DoubleClick Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).
7. Google is defending an additional wiretap class action, Google, Inc. Privacy Policy Litig., 12-cv-01382-PSG (N.D. Cal.), related to Google's decision to unify the privacy policies of all Google platforms and to co-mingle data.
8. Co-author D. Straite has been court-appointed to a committee advising lead counsel for the plaintiffs on this appeal.
9. 5:12-md-02314-EJD (N.D. Cal.).
10. Nickelodeon Consumer Privacy Litigation, MDL 2443 (D.N.J.).
11. The authors are co-counsel to the Plaintiffs in the PulsePoint litigation.
12. PulsePoint has moved to transfer the case to Delaware to be consolidated and/or coordinated with the Google case. The motion is pending.
13. 5:13-md-02430 (N.D. Cal.).
14. Google Inc. Gmail Litigation, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013).
15. Google Inc. Street View Elec. Comm. Litig., 10-cv-02184-JW (N.D. Cal.).
16. Aff'd sum nom., Joffe v. Google, Inc., 729 F. 3d 1262 (9th Cir., 10 Sept 2013).