

SUPREME COURT OF VICTORIA

COURT OF APPEAL

S APCI 2009 3860

AUSTRALIAN STYLE PTY LTD  
(ACN 099 892 814)

Appellant

v

.au DOMAIN ADMINISTRATION  
LIMITED (ACN 079 009 340)

Respondent

---

JUDGES

BUCHANAN, WEINBERG and HARPER JJA

WHERE HELD

MELBOURNE

DATE OF HEARING

18 February 2010

DATE OF JUDGMENT

23 July 2010

MEDIUM NEUTRAL CITATION

[2010] VSCA 184

JUDGMENT APPEALED FROM

[2009] VSC 422 (Hargrave J)

---

CONTRACT - Domain name registrar agreement between registrar and regulator - Whether 'security breach' of registrar's system - Failure by registrar to provide immediate notification of breach to regulator - Whether termination of agreement open to regulator - Whether 'security breach' only arises where unauthorised access to confidential, personal registrant data occurs - Whether breach could be retrospectively authorised - Necessity to maximise protection of registrants and to maintain confidence in domain name system as a public resource - Regulator to exercise its responsibilities in good faith - Breach not capable of remedy - Whether registrar acted in bad faith by transferring registrants to another entity without authorisation - Whether registrar acted in bad faith when providing notice to its registrants of the breach - Whether intermediate appellate court required to deal with all grounds of appeal - *Kuru v New South Wales* (2008) 236 CLR 1 applied.

---

Appearances:

Counsel

Solicitors

For the Appellant

Dr C L Pannam QC with  
Mr G Bigmore QC and  
Mr M J Hoyne

Mills Oakley

For the Respondent

Mr J Gleeson SC with  
Mr A Woods

Maddocks

BUCHANAN JA:

1 I agree with Harper JA.

WEINBERG JA:

2 I agree for the reasons given by Harper JA that this appeal should be dismissed.

HARPER JA:

3 It is the everyday task of the courts, when both the facts and the conclusions to be drawn from them are in dispute, to make such findings, based on the evidence, as are necessary to decide the issue or issues according to law. Since the truth is elusive, and often multi-faceted, this exercise is generally made feasible only by the rules governing the burden of proof, the drawing of inferences, and the responsibility of introducing evidence.

4 But there are exceptions. Sometimes, even in the midst of hard-fought litigation, it is relatively easy to distinguish fact from fiction, and to draw conclusions about which one can be as confident as, in human affairs, it is ever possible to be. And when one asks why the losing side fought against the odds as it did, the answer may be that litigants, as with humans more generally – their vision obscured by self-interest – sometimes convince themselves, and hope to convince others, that what is incontrovertible is not only open to challenge, but is the opposite of the conclusion which ought to be drawn. Now and again this phenomenon provides nice examples of the proposition that it is frequently easier to detect falsity than it is to discover the truth.

5 These reflections were prompted by this appeal. The present appellant, the plaintiff below, sought to persuade the trial judge that what on careful examination was clearly one thing, was actually another. His Honour was not persuaded.

He was right to have resisted the appellant's importunings. Yet this appeal has been brought. It, like the original application, must be dismissed.

6           The parties are participants in the system which governs the allocation and use of internet domain names. It is a system which is now an essential part of daily life, including daily commerce. Those who transact their business and other affairs over the internet depend upon it being secured against those who would exploit it, and the information it contains, in order to obtain an unlawful financial or other advantage. Protecting the system against unauthorised entry is therefore of paramount concern. Both parties to the present litigation had an obligation to maintain that security. One of them, the appellant, failed in this duty.

7           The courts and the lawyers also must play their part in the maintenance of the .au domain name system as an important public resource. But it is worth making the point that in this endeavour less may sometimes mean more: the end will not necessarily be best promoted by the taking of an unduly legalistic approach. The principal responsibility for management of the internet must be reserved to those with the relevant expertise; those, in other words, who are familiar not only with what the internet now is (in all its intricacies) but also with what it might become. The law can sometimes, no doubt, assist from the wings. It also has the potential to meddle, both from the periphery and from centre stage. It *will* meddle, unless the lawyers and the courts approach with diffidence whatever limited role they have.

8           The ultimate responsibility for the efficient administration of the internet domain name system lies with the Internet Corporation for Assigned Names and Numbers ('ICANN'), which is based in California. In Australia, following endorsement by the Commonwealth Government, a not-for-profit corporation named (in a style befitting its place in the scheme of things) '.au Domain Administration Ltd' ('auDA'), was appointed by ICANN as the administrator of .au domain names.

9           Very properly, the Commonwealth’s endorsement was conditional. In a written statement submitted to ICANN, the Commonwealth confirmed that its endorsement of auDA as administrator was subject to auDA demonstrating its ability to: (i) be inclusive of, and accountable to, members of the internet community; (ii) enhance benefits to internet users through the promotion of competition, fair trading and provision for consumer protection and support; and (iii) represent the Australian internet industry. The Federal Government’s letter of endorsement goes on to record that the .au domain name system is a public resource to be administered in the public interest. Accordingly, the Government retains for itself the ultimate authority for the management and administration of .au domain names. Indeed, under the *Telecommunications Act 1997*, reserve powers are conferred upon Commonwealth agencies to take control of, and oversee electronic addressing of, .au domain names.<sup>1</sup> In addition, auDA’s conditions of appointment required it ‘to administer the .au domain name system for the benefit of the Australian internet community’ and ‘in the interests of the global internet community.’<sup>2</sup>

10           These names are marketed and sold by registrars, each of which has entered into a standard form of ‘registrar agreement’ with, and has been accredited by, auDA. Their customers or clients are known as registrants. The appellant, Australian Style Pty Ltd (‘Australian Style’), which uses the trading name ‘Bottle Domains’ was and is a registrar. It is also a member of a group of companies – each of them registrars in their own right – to which I shall refer as the “Bottle Group”.

11           The appellant was appointed on 8 August 2002, pursuant to an agreement (‘the registrar agreement’) with auDA. Clause 14.1 of that agreement imposes a number of positive obligations upon Australian Style as registrar. By that clause, Australian Style must:

14.1.1   act in good faith in its dealings with auDA ...;

14.1.2   do all things necessary to ensure that ... it continues to meet the accreditation criteria;

---

<sup>1</sup>        *Telecommunications Act 1997* (Cth), Part 22, Division 3, ss 475–476.

<sup>2</sup>        Judgment below, [8].

- 14.1.3 immediately give auDA notice of any security breaches affecting the Registrar or any part of its systems.

12 The agreement also imposes obligations upon auDA. These affect its role as administrator of the .au domain name system, and the exercise by it of its powers and duties under agreements with registrars; and they reflect its position as a body required to make the protection of the public interest its primary consideration in what it does and how it does it. Clause 19.1 is, in this context, especially relevant. Consistently with the Commonwealth Government's letter of endorsement, and with auDA's duty to administer the .au domain name system as a public resource for the public benefit, clause 19.1 provides that auDA must, in relation to all matters that impact upon the rights, obligations or role of Australian Style:

- 19.1.1 exercise its responsibilities in good faith and in an open and transparent manner; and
- 19.1.2 not unreasonably restrain competition and, to the extent possible, promote and encourage robust competition; and
- 19.1.3 not apply standards, policies, procedures or practices arbitrarily, unjustifiably, or inequitably; and
- 19.1.4 not single out [Australian Style] for disparate treatment unless justified by substantial and reasonable cause; and
- 19.1.5 ensure, through its reconsideration and independent review of policies, adequate opportunity for [Australian Style] to contribute to auDA's standards, policies, procedures or practices.

13 Given the events which gave rise to this litigation, clause 23 is also of particular relevance. It (rather awkwardly) defines an 'Event of Default' as:

- 23.1.1 an insolvency event; or
- 23.1.2 the registrar [Australian Style] does not continue to meet the accreditation criteria; or
- 23.1.3 any amount due and payable by [Australian Style] under this document is in arrears for 30 days after formal demand has been made; or
- 23.1.4 [Australian Style] commits a breach of this document which is not capable of being remedied; or
- 23.1.5 [Australian Style] commits a breach of this document and fails to rectify that breach within 30 days after receipt of written notice specifying the breach and requiring rectification.

14            Clause 4 of the registrar agreement is headed 'Loss of Registrar's accreditation.' Clause 4.2 provides that auDA may suspend or terminate Australian Style's accreditation if it considers that a relevant event of default has occurred. Additional powers conferred on auDA in the event of a default are specified in clause 23.2 of the agreement. Clause 23.2.5 empowers auDA to terminate that agreement by notice in writing given at any time following an event of default. But this power is subject to the general obligations imposed upon auDA by clause 19.1. Furthermore, if the relevant breach is capable of being remedied, auDA may not terminate unless (a) a 30 day notice pursuant to clause 23.1.5 has been served, and (b) the breach has not been remedied within that period.

15            Of all the obligations placed upon a registrar, that which requires the immediate notification to auDA of any security breaches affecting the registrar or any part of its systems is clearly of especial significance. auDA asserts that Australian Style was the victim of such a breach, but failed to tell auDA about it. auDA took the view that this amounted to a failure to honour the obligation, imposed upon Australian Style by clause 14.1.3 of the registrar agreement, immediately to give auDA notice of any security breaches affecting it or any part of its systems. Furthermore, according to auDA, that failure was not only itself a breach of that clause, but was a breach incapable of remedy. auDA therefore terminated the agreement, and withdrew Australian Style's accreditation as a registrar. Australian Style then issued proceedings to challenge the termination, and to enforce its claimed entitlement to continue to operate as a registrar. It asserted that no breach had occurred; but even if it had, it was (so Australian Style contended) capable of being remedied. Clause 23.1.5 required that Australian Style be given 30 days to effect that remedy. This it had been wrongfully denied.

16            Hargrave J delivered judgment following a trial the hearing of which occupied six days. His Honour found that, in or about April 2007, Australian Style had been the victim of what the judge initially referred to as a 'security incident', but which he later held to be a security breach within the meaning of that expression in

clause 14.1.3 of the registrar agreement. Australian Style failed to give auDA immediate notice of this breach although, in his Honour's judgment, such notice was required by that clause because the consequence of the incident was that the vulnerability of one or more of the appellant's systems was exposed (and so, to adopt a cognate term to that employed in clause 14.1.3, "affected"). His Honour further held that this was a breach which was not capable of being remedied. It therefore fell within clause 23.1.4 of the registrar agreement. For these reasons, auDA was entitled – if not bound – to terminate the agreement. It is these findings which form the basis of grounds 1-4 of Australian Style's grounds of appeal.

17           It is helpful to view the appeal in context and then, with that context in mind, to examine the grounds of appeal. I begin this part of the exercise by noting that the April 2007 security breach which, according to auDA, led to its decision to de-register Australian Style, was first brought to its notice early in 2009. This was after the Australian Federal Police had notified auDA of another, and undoubted, security breach in which the database of Australian Style, including domain name passwords and credit card details of its registrants, had been offered for sale on the internet.

18           The AFP asked auDA to keep this information, and the fact of the police investigation, confidential. In compliance with this request, the Chief Executive Officer of auDA (Mr Christopher Disspain) did not bring the matter to the appellant's attention. He merely arranged to have all of those domain names which were managed by Australian Style monitored for any unusual activity. Then, on 5 February 2009, the AFP made an arrest. This was the trigger for Nicholas Bolton, who owns and controls Australian Style, to be told by the police of their investigations, of the consequential arrest, and of their reasons for their actions.

19           Following this, at 8.15 that evening, Mr Bolton emailed Mr Disspain. He included in the email a note that he would be available 'at any time' to discuss the matter. It is perhaps symptomatic of Mr Bolton's subsequent conduct of himself and his organisation that, despite this indication, Mr Disspain's attempts to contact him that evening by telephone were fruitless.

20           A meeting was, however, held the next day, 6 February. Mr Bolton, in an affidavit sworn on 16 April 2009, deposed that he then informed auDA that the unauthorised access which enabled the making of the offer to sell the database ‘may have been obtained through the vulnerability which was exposed in April 2007.’ He added:

Based on the evidence now at hand, it appears that this data the subject of investigation by the AFP was, in fact, obtained as part of the accessing of the information by Aust Domains in April 2007.

21           Whatever exposure there may have been during the course of that year, auDA knew nothing of the 2007 ‘accessing of ... information by Aust Domains’ until, some 21 months later, the meeting of 6 February 2009 was held. More details were provided by Mr Bolton in his affidavit of 16 April 2009. He there described the April 2007 incident as arising out of the relationship between Australian Style and one of its competitors, Aust Domains International Pty Ltd. The latter is another accredited registrar of domain names. In 2004, it was licensed by Australian Style to use for its own management purposes the software by which Australian Style managed those .au domain names for which the appellant was the registrar of record.

22           On 10 April 2007, the Chief Executive Officer of Aust Domains contacted Mr Bolton by telephone. What happened next is the subject of paragraphs [18]–[22] of Mr Bolton’s affidavit:

[18]   On 10 April 2007 I received a telephone call from ... the CEO of Aust Domains who informed me that:

- (a)   Aust Domains had employed a software developer to review the source code and through this review he had identified a vulnerability in the system that they used under licence, in that he was able to access ... and download a ‘table structure’ from the system. A table structure is simply, as the name suggests, the format or structure of a table. It does not contain any data;
- (b)   as [Australian Style] also used the same system, the developer attempted to access [Australian Style’s] system to identify if it also had a similar vulnerability;
- (c)   he had identified that [Australian Style] did in fact have the same vulnerability; he claimed that he obtained only non confidential data in our system to verify the vulnerability. There was no indication that any sensitive consumer data was

obtained;

- (d) Aust Domains had developed a 'patch' to fix the security flaw and could provide that to [Australian Style] for a fee; and
- (e) during that call [the CEO] gave me an undertaking that Aust Domains had destroyed all material obtained by reason of the access of [Australian Style's] system.

[19] [Australian Style] subsequently obtained the patch from Aust Domains and applied it to its system. Aust Domains provided the patch free of charge pursuant to the Software Agreement.

[20] There is no evidence to suggest that the patch applied at that time was unsuccessful in fixing the security flaw and to the best of my knowledge no other unauthorised access has been made by any party.

[21] At the time, I did not consider the above events to constitute a 'security breach' (whatever that phrase may mean) for the following reasons:

- (a) it was only through the extensive knowledge and experience of Aust Domains in using the similar software that allowed it to identify the security flaw in its, and [Australian Style's], systems. Accordingly, it was extremely unlikely that an external party would have been able to gain access to [Australian Style's] systems given the significant level of knowledge required;
- (b) it was my understanding that the only information obtained by Aust Domains was 'table information data' which was merely system data and not in any way confidential nor related to [Australian Style's] customers' personal details;
- (c) in effect, Aust Domains had simply identified a security flaw in our system [which we were previously unaware of] and provided the means by which that flaw could be remedied;
- (d) Aust Domains gave undertakings [that] the information which it obtained had been destroyed;
- (e) even if Aust Domains had obtained confidential information it would be bound by the confidentiality agreement contained in the Software Agreement as well as the obligations of non disclosure of confidential information by virtue of being an accredited registrar; and
- (f) [Australian Style] was able to obtain and immediately apply a patch to the system to prevent any further access.

[22] In those circumstances, it was my view that there was no obligation on [Australian Style] to notify auDA of these events because there had not been a 'security breach'.

23 In his oral evidence before Hargrave J, Mr Bolton said that the 'security flaw' could be exploited through a web browser, and that such exploitation is referred to as a 'PHP injection'. He added:

We believe the flaw was the ability of someone with intimate knowledge of our software to insert a very specific code into a form on our website that would return results to them. So with the knowledge of what code to write and where to look within our system they were able to return data back to them and that may [be] nonsensical data or it may be other data.

24 In these extracts from Mr Bolton's affidavit and oral evidence, he refers to the possibility that the access which constituted the 2009 breach (and the resultant offer to sell Australian Style's database) 'may have been obtained through the vulnerability which was exposed in April 2007.' He also refers to 'the systems' employed by Australian Style and Aust Domains; to their 'vulnerability'; to the verification of that vulnerability by Aust Domains' ability to extract data from within the 'system'; to steps taken to 'fix' the 'security flaw' thus revealed; to the extreme unlikelihood (but, therefore, to the possibility, however remote) 'that an external party would have been able to gain access to [Australian Style's] systems'; and to Aust Domains' assertion that the information it obtained had been destroyed - an unnecessary step if it was unquestionably innocuous, or (in other words) 'merely system data and not in any way confidential nor related to [Australian Style's] customers' personal details'.

25 All of this tends to support the proposition that a security breach had occurred. Consistently with the possibility that an external party may have been able to gain access to the appellant's systems, and to confidential data stored there, Aust Domains 'claimed' that no confidential information had been obtained, and that what had been obtained had been destroyed - while the appellant adopted the position that, if this was not so, Aust Domains would be bound by its confidentiality agreement (and so no confidential information would be further disseminated). It is therefore no wonder that Australian Style thought it prudent to change the passwords which gave access to its private data (although it did not change the passwords of its registrants because - as it claimed in an explanation which his

Honour described as ‘wholly unsatisfactory’ – Mr Bolton believed that they had not been accessed.<sup>3</sup> Yet the appellant continues to insist that what Mr Bolton described was not a security breach. Here lies the wonder.

26

It is these circumstances, among others later to be examined, which gave rise to the reflections with which this judgment began. At paragraphs [159]–[162] of the judgment below, his Honour contrasted the starkly opposing positions taken by the parties in relation to the 2007 incident. He did so in terms which seem to me to nicely illustrate the lack of reality in the stance of the appellant:

[159] Mr Disspain’s belief that Mr Bolton had not acted in good faith ... was also motivated by a belief that Mr Bolton’s conduct, when considered as a whole, demonstrated that he did not understand the seriousness of the 2007 security incident and his failure to give immediate notice of it to auDA. Mr Disspain’s belief in this regard was based upon a consideration of the conduct of Mr Bolton concerning the 2007 security incident and in response to the 2009 security breach. The following principal matters informed his belief.

[160] First, Mr Disspain had a clear view that the 2007 security incident constituted a security breach within the meaning of clause 14.1.3. His view was confirmed by discussions with relevant auDA staff and [another relevant person]. He could not understand how Mr Bolton could hold a contrary view. To Mr Disspain, once he learned on 13 February 2009 that the Aust Domains consultant had penetrated the Australian Style database and downloaded information, there was no credible argument that a security breach had not taken place. The fact that Mr Bolton did not understand this, and wished to argue that there was a mere unexploited security vulnerability, indicated to Mr Disspain that Mr Bolton did not understand the seriousness of a security breach and the fundamental need for auDA to be informed as soon as a registrar becomes aware of a security breach.

[161] It was submitted on behalf of Australian Style that it was totally unreasonable for Mr Disspain to give no credibility whatever to the contrary view expressed by Mr Bolton. I do not accept that submission. Mr Disspain’s view that the 2007 security incident constituted a security breach was correct. ...

[162] Second, accepting the truth of what Mr Bolton had told auDA concerning the 2007 security incident and Australian Style’s response to it, Mr Disspain considered that the conduct of Australian Style demonstrated that it did not treat the 2007 security incident with sufficient seriousness. Mr Disspain’s concerns in this regard were stated in the notice of termination by auDA of the registrar agreement, and expanded upon in his affidavit sworn in opposition to the application for an interlocutory injunction.

---

<sup>3</sup> Judgment, [19].

27           Given the importance of the .au domain name system as a public resource to be administered in the public interest, it is in my opinion appropriate that this Court say clearly that it endorses the approach taken by Mr Disspain, and therefore also his Honour's approval of it.

28           Mr Bolton's attitude is the more inexplicable given that on 6 February 2009 he was informed, by an email from the Australian Federal Police, of its belief that the database was accessed not only on 27 January that year, but also on 30 June 2008; that all of the database, together with the credit card numbers held there, may have been compromised; and that failure to provide credit card numbers to the issuing banks would be 'an unacceptable risk'. There is nothing in the evidence to explain how the AFP could come to these conclusions when Australian Style either could not or would not.

29           Mr Bolton was more in touch with reality when (as recorded in a letter dated 16 February 2009 from auDA's solicitors to the solicitors for Australian Style) he said in a teleconference held on 13 February that 'the [April 2007] security breach arose from an unauthorised person gaining access to [Australian Style's] systems, and, result[ed] in that unauthorised person downloading and obtaining data - to which the unauthorised person was not entitled to download or obtain - from [Australian Style's] systems or database.' Here was a security breach. Mr Bolton was right to categorise it as such.

30           One final piece of evidence relevant to this aspect of the present appeal is that, at some point, Mr Bolton granted retrospective authorisation to Aust Domains to do what it did when, in April 2007, it downloaded Australian Style's 'table structure'. According to Australian Style, this ex post facto authorisation fixed everything. If there was once a breach, it was now expunged. Indeed, it had been expunged so thoroughly that it was henceforth to be taken as never having been a breach at all.

It is against this background that the first three grounds of appeal are to be considered. They carry the heading *Clause 14.1.3 of the Registrar Agreement* and are as follows:

- 1
  - (a) His Honour erred in construing clause 14.1.3 of the [Registrar] agreement ... (which provided that the appellant must 'immediately give [the respondent] notice of any security breaches affecting [the appellant] or any part of its systems') as requiring the appellant to give 'immediate notice to [the respondent] of any circumstances resulting in an unauthorised person obtaining access to any part of the systems by which [the appellant] maintains the privacy of information kept by it concerning itself or registrants, whether or not that breach results in unauthorised access to that information'. (Paragraph [105] of the judgment)
  - (b) His Honour ought to have found that, on its proper construction and in accordance with its ordinary meaning, clause 14.1.3 of the registrar agreement meant that the appellant was required to give the respondent notice as soon as reasonably practicable after becoming aware of facts that showed that a person did gain, or could reasonably have been assumed to have gained, unauthorised access to the confidential information of registrants or the respondent.
- 2 His Honour erred by determining that the appellant knew that there had been access by an unauthorised person to some part of the systems by which the respondent maintains the privacy of information kept by it concerning itself or registrants (which finding is a necessary finding for the determination, made by his Honour at paragraph [109], that there had been a security breach and breach of clause 14.1.3) where there was no evidence, or no evidence upon which the Court ought to have proceeded, to support such a finding. That is, that the only evidence on the question of whether the computer system which Mr Bolton advised in April 2007 had been accessed via a PHP injection (per paragraphs [18] and [107]) (the 2007 incident) was 'part of the systems' by which the appellant maintained the privacy of information kept by it concerning registrants was the unchallenged evidence of Mr Bolton that the private information could not have been obtained by means of the PHP injection as described to Mr Bolton in 2007.
- 3 His Honour further erred in determining that, for the purposes of clause 14.1.3, a 'security breach' will have occurred even if the person who had gained access to the appellant's systems was authorised to do so if the express authorisation was given after access had been obtained (paragraph [110]).

The registrar agreement does not define the expression 'security breach'. The appellant suggests that this is surprising, given that such a breach triggers the

obligation to notify auDA of its occurrence, and given that a failure to notify will, or at least might, amount to an event of default which in turn will enliven auDA's draconian power to terminate Australian Style's accreditation.

33 I do not think that there is anything surprising about the failure to define a security breach. Other comparable expressions are not defined in other important documents. The constitution of the United States of America does not define the expression 'high crimes and misdemeanours', although their commission by a President could result in his or her impeachment. The Australian constitution does not define the word 'misbehaviour', although a federal judicial officer who misbehaves may be dismissed by Parliament.

34 The failure of the registrar agreement to define 'security breach' is I think a strength, not a weakness, in registrar agreements, one of the purposes of which is to enable an administrator of domain names to maintain, and ensure that those it has accredited as registrars provide, security for internet users. That security is of great, if not crucial, importance. Whether a security breach has occurred will depend on all the circumstances of the particular case; and these will differ in a myriad of ways. A clear and all-embracing definition is almost certainly beyond the realm of the possible. Yet a combination of technical expertise and common sense will generally enable both administrators and registrars to identify a security breach when they see one. They will be directly impeded in that endeavour if lawyers without the relevant technical knowledge become engaged in the identification process.

35 That engagement, however, would be inevitable were an attempt made to describe what, in the context of the internet, a 'security breach' is. The closest one can perhaps get is to say that such a breach would *probably* result whenever unauthorised activity exposed a flaw in those mechanisms whose role it is to protect confidential information. But a security breach will not necessarily occur in those circumstances, and may occur in others.

36 The submissions made by the appellant on this appeal seem to me to illustrate

the point. The appellant argues that a security breach occurs only 'where a person without authorisation (either before or after access is obtained) deliberately accesses confidential, personal data'.<sup>4</sup> This is to argue, in effect, that a security breach occurs not when the parapets succumb, but only when the raider, having breached the inner wall, enters the close. According to the appellant, unauthorised action may expose the data; but if that data is not confidential, or is not accessed, there is no breach. It follows that, if the appellant is right, six elements must be established before a security breach is confirmed. First, that there be an unauthorised activity; secondly, that by that activity an opportunity is obtained to circumvent protective mechanisms; thirdly, that the way is thereby opened to access information; fourthly, that deliberate advantage is taken of that opportunity; fifthly, that that information is confidential and 'personal' (whatever, in this context, the latter word means); and, finally, that the unauthorised activity is not subsequently sanctioned.

37           There may be some instances where it is immediately apparent that the exposure of a registrar's systems to unauthorised access is of absolutely no consequence. The concern, after all, is not with a mere breach. Two words are involved. The other is 'security'. If the breach can at once and with certainty be seen to have no effect on the security of the registrar or its systems, then it is not a breach that is caught by clause 14.1.3.

38           But, having said that administrators and registrars should be able to identify a security breach when they see one, I disavow any suggestion that this judgment (otherwise than by saying that in this case a security breach occurred) has in some way defined what a security breach is. Indeed, my point is that registrars may draw back from taking important remedial measures if, although systems have been exposed to unauthorised exploitation, some possible argument about the definition of a 'security breach' might serve as an excuse for inaction. Registrars are naturally inclined to hesitation when confronted by the realisation that their systems have been thus exposed. Such hesitation, even if inexcusable, would be understandable,

---

<sup>4</sup> Australian Style's written outline of submissions, 18 January 2010, [4].

because the adverse consequences for the registrar might be considerable. Yet it is vital that overall confidence in the .au domain name system as a public resource be maintained; and this cannot be done unless those who depend on it know that, if a security breach does occur, remedial action will be taken at once. The general rule should doubtless be: protection first, investigation later. Protection, users would doubtless agree, involves immediate notification of the potential or actual breach. The notice should go to the relevant administrator of internet domain names (in Australia's case, auDA). Time will be of the essence. There should be no stay while pin-pricking (or perhaps any) inquiries are undertaken into the genuineness of the breach, or into whether each of the definitional elements of its meaning have been met.

39            Clause 14.1.3 of the registrar agreement has a clear purpose. It is the duty of auDA to give it effect. That purpose is the protection not of registrars but of registrants. For them, the security of their interests depends upon practical effect being given to the maxim that it is better to be safe than sorry. Clause 14.1.3 must therefore be construed not as the appellant would have it – so as to minimise inconvenience to registrars – but so as to maximise the protection given to registrants.

40            The appellant takes a different approach. It submits that '[t]he supervision of security is not at the core of the relationship between the respondent and registrars.'<sup>5</sup> At least to the extent set out below, I disagree. The Commonwealth Government's endorsement of auDA as administrator of .au domain names was conditional upon it demonstrating its ability to (among other things) provide consumer protection and support. This circumstance forms part of the matrix of facts against which the registrar agreement is to be construed, because the appellant as a responsible registrar is to be taken to have known, at least in broad terms, what the responsibilities of auDA are. Seen in this light, the requirement imposed upon Australian Style by clause 14.1.3 – that is, to give auDA immediate notice of any

---

<sup>5</sup> Appellant's outline of submissions, 18 January 2010, [11].

security breaches, with failure to do so being an event of default under clause 23.1.4 – must in my opinion be taken to be at the core of the relationship between appellant and respondent.

41           The appellant contends that if this conclusion is accepted then ‘if a registrar honestly but wrongly forms the view that an incident is not a security breach (and so does not report it) then it is unable to remedy that breach and the registrar is liable to have its business (which it may have built up over many years and spent a lot of money in developing) unilaterally terminated by the respondent.’ ‘That’, the submission continues, ‘is a good reason to adopt a narrower construction of “security breach”.’<sup>6</sup>

42           Again, I disagree. The court must proceed on the basis that auDA will adhere to the requirement, imposed by clause 19.1.1 of the registrar agreement, that it exercise its responsibilities in good faith. The Court is therefore entitled to assume that auDA will not terminate a registrar agreement for an honest mistake unless some aspect of the mistake – such, for example, as it being induced by a failure to properly regard the interests of registrants – indicates that termination is appropriate.

43           This answers, in part, another submission advanced by the appellant. At [13] of its outline of submissions of 18 January 2010, the appellant contends that:

If the failure to notify a security breach may result in termination of a registrar agreement, the registrars will adopt a ‘conservative approach’ and the class of incidents which registrars will be reporting will become absurdly wide. Registrars may take the view that every time they receive a notification ... that a security patch is being released then they should notify the respondent because there is the potential that someone may have gained access to that flaw. This will render the process largely pointless as well as adding considerably to the administrative workloads of registrars and the respondent (resulting in increased domain name fees).

This submission was supplemented orally on the appeal by the contention that, if a wide definition of the expression ‘security breach’ were adopted, the appellant would be required to report every attempt to hack into its system, which would be a

---

<sup>6</sup> Appellant’s outline of submissions, 18 January 2010, [12].

daily occurrence.

44           These submissions assume that registrars lack common sense, and that auDA will act tyrannically. Neither assumption should be adopted by this Court. Notification that a security patch is being released does not of itself necessarily imply that a security breach has been detected. It may indicate no more than that by some authorised activity a vulnerability (it may be merely a potential vulnerability) has been discovered. And a wholly unsuccessful attempt to hack into a system will not amount to a security breach. Moreover, auDA is required by clause 19.1.1 of the registrar agreement to exercise its responsibilities openly and transparently, and by clause 19.1.3 to apply standards justly and equitably. Together, auDA and its registrars should be able to avoid any prospect of ‘the class of incidents which registrars will be reporting [becoming] absurdly wide.’

45           In his oral submissions on the appeal, senior counsel for the appellant posed the rhetorical question: what would the respondent have done had it been notified? I agree with the trial judge in accepting the evidence of Mr Disspain that it would have acted in much the same way as it did in 2009; and even without Mr Disspain’s evidence, the answer could be inferred by reference to what auDA did when notified of the 2009 breach. Amongst other things, it sent emails to the appellant’s registrants, telling them what happened. It required the appellant to do the same. Its power to so require was not questioned then, and one may suppose that the appellant would have taken a like position in 2007, had auDA been involved at that time. Had the appellant challenged auDA’s authority, that challenge may have been answered by reference to the power of auDA to issue accreditation criteria as occasion requires. Failure to meet the accreditation criteria is an event of default: clause 23.1.2.

46           If the approach indicated in the preceding paragraphs of this judgment is correct in principle, then a security breach can occur without there being actual access to confidential information. In this case, a software developer employed not by the appellant but by Aust Domains identified a vulnerability in the appellant’s

software. The software developer, although not authorised to do so, then exploited that vulnerability. As a result, information (Australian Style's table structure) was obtained. The appellant asserts that that information was not confidential, and that the fact of the vulnerability and its exploitation was therefore inconsequential. Hence the second ground of appeal – that there was no evidence to support his Honour's finding that Australian Style knew of the (unauthorised) access 'to some part of the systems by which the [appellant] maintains the privacy of information kept by it concerning itself or registrants'.

47           The appellant's own evidence, however, eloquently puts the contrary case. It demonstrates, in my opinion, that even if a security breach only occurs when the data accessed is confidential, in this case confidential information was – or at least in the assessment of the appellant might have been – exposed.

48           Mr Bolton himself described what was revealed in April 2007 as both a 'security flaw' and a 'security breach'. In the words which he used in his affidavit of 16 April 2009, this amounted to a 'vulnerability in the system' enabling Aust Domains to gain access to that system. Australian Style's reaction was to treat this as a security breach – the only exception being that clause 14.1.3 was ignored in the process. The appellant clearly believed that the unauthorised access by the software developer to the appellant's system might have extended to access to confidential information held within that system. So it changed its password, and obtained an undertaking from Aust Domains that all material obtained by the latter's exploitation of the vulnerability had been destroyed. Then it acquired a patch 'to fix the security flaw'.

49           The change to Australian Style's password is, it seems to me, especially significant. As the trial judge remarked at paragraph [123] of his judgment, Mr Bolton acknowledged that he did this as a matter of prudence, in order to avoid the risk of unauthorised access to Australian Style's private information. Having secured his own perimeter, he nevertheless neglected to protect those for whose protection the appellant was responsible; and he failed satisfactorily to explain why.

50           The necessary conclusion is that the appellant realised that there was a flaw, that confidential data was thereby put at risk, and that at least some remedial action was required. This conclusion is strengthened by Mr Bolton's concession that the unauthorised access of early 2009 'may have been obtained through the vulnerability which was exposed in April 2007.' In my opinion, his Honour was correct in finding that the 2007 incident clearly amounted to a security breach.

51           If the above conclusions are correct, then grounds 1 and 2 of the grounds of appeal are not made out.

52           Ground 3 of the grounds of appeal is to the effect that his Honour was wrong to conclude that authorisation may not be given retrospectively. Whatever might be the position in other circumstances - and about them I say nothing - in the circumstances of this case retrospective authorisation was not open to the appellant. The imperative dictated by clause 14.1.3 is immediate notification to auDA of an actual or possible breach of security. The issue is not one between a registrar and the entity gaining access (which access is unauthorised at the time, but which the registrar might authorise after the event). The issue is between the registrar and auDA. Once unauthorised access has, to the knowledge of a registrar, been gained or possibly been gained, the registrar must notify auDA. That obligation is, and must be, in the here and now. It cannot be fulfilled by the action of the registrar in subsequently giving 'authorisation' to an entity which once lacked it. Indeed, the approach advanced by the appellant fails to appreciate that the interests which must be protected are the integrity of the internet and the interests of its users. There is no place in this scheme of things for an individual registrar, acting in and for its individual interest, to authorise after the event actions which, unknown to it, may have had adverse consequences for other parties with a legitimate stake in the proper functioning of the domain name system as a public resource.

53           The fourth ground of appeal appears under the heading *Breach Capable of being Remedied*. It reads:

- 4 (a) His Honour erred in determining that the failure of the appellant to give notice to the respondent of the 2007 security incident was not theoretically capable of being remedied. (Paragraph [119]).
- (b) His Honour ought to have determined that, if the 2007 security incident was in breach of clause 14.1.3 of the registrar agreement, then such breach was capable of being remedied and the registrar agreement could not be terminated without a notice of breach being served in accordance with clause 23.1.5 of the registrar agreement.

54 In my opinion the answer to this ground is to be found in the use in clause 14.1.3 of the word 'immediately'. It is central to the obligation which that clause imposes. It means what it says. An opportunity to give immediate notice, once lost, cannot be regained; and therefore, in this sense, cannot be remedied. In some circumstances this would not matter, because the purpose behind the requirement for immediate notice can be achieved even though that requirement has not been met. That, however, is not – or will not – be generally true in the circumstances which clause 14.1.3 is designed to meet. Its object is to ensure that, in a situation in which time can be expected to be of the essence, auDA is given a timely opportunity to determine upon remedial action – and then take it. As Lord Reid said in his speech in *Wickman Tools v Schuler A.G.* 'there are cases where it would seem a misuse of language to say that a breach can be remedied.'<sup>7</sup>

55 The trial judge provided in clear terms in paragraphs [111]–[126] of the judgment below additional reasons why ground 4 must fail. It is convenient to reproduce paragraphs [120]–[126], which begin with the first of his Honour's reasons for holding, correctly, that the breach by Australian Style of its obligation under clause 14.1.3 to give immediate notice of the 2007 security incident was not capable of remedy. His Honour said:

[120] First, the registrar agreement distinguishes between breaches which are capable of remedy and those which are not. Accordingly, the registrar agreement recognises that not all breaches are capable of remedy. This is plain from the structure of clauses 23.1.4 and 23.1.5.

---

<sup>7</sup> [1974] AC 235, 250.

- [121] Second, whether or not a particular breach is capable of remedy must be judged by reference to the purpose of the registrar agreement as a whole, and clause 14.1.3 in particular. As appears above, the general purpose of the registrar agreement was to permit Australian Style to conduct a registrar business subject to the terms and conditions stated, including the primary requirement that Australian Style must comply with auDA's published policies, code of practice and accreditation requirements as in force from time to time, and thus subject itself to the general regulatory supervision by auDA of the .au domain name system. The specific purpose of clause 14.1.3 was to provide auDA with a timely opportunity to consider what, if any, steps should be taken to perform its regulatory role. In this context, clause 14.1.3 is an important provision. The word 'immediately' has been deliberately chosen, and may be contrasted with the period of two business days notice specified in clauses 14.1.4, 14.1.6 and 14.1.10 of the registrar agreement. The importance of urgent notice is left in no doubt.
- [122] Third, the breach by Australian Style had the result of defeating the purpose of clause 14.1.3. In the events which transpired, auDA did not learn of the security breach arising from the 2007 security incident until nearly two years after it had occurred. The result of the breach by Australian Style was to deprive auDA of the opportunity to perform its regulatory role in 2007. auDA cannot be put in that position retrospectively. For example, Mr Disspain gave evidence that, if auDA had been given immediate notice of the 2007 security incident, auDA would then have acted in much the same way as it did in 2009. It would have suspended the Australian Style EPP connection. It would have ensured that registrants' passwords were changed. It would have ensured that registrants were informed of the possibility that their private information may have been, or may be, the subject of unauthorised access. It would have requested Australian Style to commission a security assessment, such as that undertaken by Vectra. I accept Mr Disspain's evidence in this regard. Further, I find that it is likely that Australian Style would have agreed to auDA's request to commission an independent security assessment. Had such an assessment been undertaken in 2007, the experts agreed that it would have disclosed the significant vulnerabilities in the Australian Style computer systems which were identified in the Vectra report this year. It is likely that Australian Style would have sought to comply with recommendations to remove the vulnerabilities from its computer system or to reduce them, as it has done this year – for itself and related registrars in the Australian Style [Bottle] Group.
- [123] Had auDA and Australian Style taken the above steps in 2007, the downloading of the Australian Style database by an unauthorised person, and the subsequent attempts to sell that database over the internet, may have been avoided altogether. Although the evidence is not clear as to when the unauthorised download took place, the person who offered the Australian Style database for sale on the internet represented that it was downloaded on 20 June 2008 and again on 27 January 2009. It appears that this person was not the person who downloaded the database, but an accomplice. However, even if the unauthorised download in fact took place in April 2007, prior to notice being given of the 2007 security incident to Mr Bolton,

changing the passwords of registrants at this time would have protected them against the risk of unauthorised access to their private information. As appears above, Australian Style changed its own password soon after Mr Bolton received notice of the 2007 security incident. Mr Bolton acknowledged that he did this as a matter of prudence, in order to avoid the risk of unauthorised access to Australian Style's private information. He had no satisfactory explanation as to why he did not think it was necessary for this basic step to be taken in respect of all Australian Style registrants.

[124] Fourth, it is in my view a misuse of language to say that a failure to give immediate notice of a security breach, for the purpose of providing auDA with a timely opportunity to take appropriate action to protect users of the .au domain name system, can be remedied by giving notice nearly two years after the event.

[125] Australian Style gave express consideration to whether notice was required. Mr Bolton determined that it was not. In reaching that conclusion, he was wrong. Were it not for the 2009 security breach, it is obvious that Australian Style would never have informed auDA of the 2007 security incident. In these circumstances, it is not now open for Australian Style to argue that its deliberate failure to give notice is capable of remedy some two years after the event.

[126] It was further submitted on behalf of Australian Style that the purpose of the notice requirement in clause 14.1.3 is to avoid actual harm being suffered by registrants as a result of unauthorised access to their private information. Accordingly, it was submitted that any security breach is capable of being remedied if the required notice is ultimately given to auDA before any harm is in fact suffered by registrants. I reject this argument. The purpose of clause 14.1.3 is to provide immediate notice to auDA of security breaches. The steps which auDA may determine are necessary as a result of receiving notice are not limited to ensuring that Australian Style registrants do not suffer harm. auDA has a wider responsibility, to the whole of the Australian internet community. It would be inconsistent with the underlying purpose of the registrar agreement and clause 14.1.3 in particular to treat the breach by Australian Style as one which was capable of remedy. After all, the requirement is only to give notice.

56 I respectfully adopt these reasons.

57 Given that the appellant has failed on each of the first four grounds of appeal, the appeal must be dismissed. But there were before the Court three other grounds, and auDA's notice of contention. Ground 5 of the grounds of appeal was not pursued, and there is accordingly no need for it to be considered here.

58 Grounds 6 to 8 concerned findings made by his Honour on an alternative case put by auDA as further justification of its termination of the registrar agreement.

That case was to the effect that the appellant acted in bad faith when it unilaterally disturbed the status quo which the Court, by orders made on 16 April 2009 and 22 April 2009 by, respectively, Hansen J and Judd J, intended to preserve. The appellant thereby demonstrated a lack of good faith.

59           The trial judge briefly expressed his views on this aspect of the case. Brevity was appropriate because his finding that the appellant had committed a breach of clause 14.1.3 which had not been and could not be remedied made it strictly unnecessary to go further. On appeal, that issue, and those raised by the notice of contention, would be relevant only if his Honour erred in this conclusion. In these circumstances, it is (as the High Court pointed out in *Kuru v New South Wales*)<sup>8</sup> necessary to consider whether to deal with all these matters in addition to those grounds of appeal which have been identified as decisive.

60           That exercise involves, first, an assessment – so far as possible – of the likelihood of there being a grant of special leave; and secondly, an assessment, if special leave were to be granted, whether the High Court would deal with the matters raised in any notice of contention (and such a notice has been filed in this appeal) or, instead, remit those to this Court. The cost consequences of these alternatives should also be considered.<sup>9</sup> Finally the Court is entitled to take into account its own workload. There is, after all, no point in expending scarce resources in the creation of obiter dicta which, even in the event of an appeal to the High Court, are unlikely to assist anyone.

61           It is, I think, unlikely that an application for leave to appeal to the High Court would be granted. But if it were, and if the appeal succeeded, it is almost certain that the outstanding issues would be remitted to this Court. Moreover, there may be some benefit in the Court giving its opinion of the behaviour in which the appellant, a registrar whose role it is to assist in the administration of a public resource, engaged. In these circumstances, it seems to me to be appropriate to examine not

---

<sup>8</sup> (2008) 236 CLR 1; (2008) 82 ALJR 1021; 256 ALR 260, [12].

<sup>9</sup> See *Health World Ltd v Shin-Sun Australia Pty Ltd* [2009] FCR 218, [47] (Perram J).

only grounds 6-8, but also some aspects of auDA's notice of contention. I begin with ground 6.

62           Following auDA's termination of the registrar agreement, and at its direction, all of the appellant's registrants were transferred to auDA. This was intended to be a temporary measure: auDA planned a further transfer when new registrars of record, acceptable to the registrants, could be found. But before that could happen, Australian Style obtained the intervention of the Court. On 16 April, Hansen J granted the appellant's application for an interim injunction requiring the reversal of the transfers. On 22 April, Judd J extended this injunction until the hearing and determination of the proceeding or further order. The result was the reversal of the transfers by the return to Australian Style of its registrants and, as the trial judge found, a renewed mandate in Australian Style 'to continue carrying on its registrar business pending determination of this proceeding.'

63           The appellant, however, had other plans. They involved it ceasing, or at least drastically reducing, its registrar business. In May 2009, Australian Style joined with another member of the Bottle Group (Bottle Domains Pty Ltd) in transferring to the latter about 95% of the domain names which, as a consequence of the injunctive relief obtained by the appellant, had not long before been re-transferred to it from auDA. This was not a move that impressed the trial judge. He said of it:

[183] The obvious purpose of the injunctions was to preserve the status quo pending determination of this proceeding. As appears below, Australian Style acted to unilaterally disturb that status quo, without notice to auDA or the sanction of the Court. Further, its actions in doing so were in breach of auDA's published policy regarding transfers between registrars.

...

[185] None of the registrants was consulted in advance of the unauthorised transfers ... [and] Australian Style engaged in this conduct without giving prior notification to the defendant or the Court.

[186] The obvious purpose of the unauthorised transfers was to defeat the efficacy of auDA's termination of the registrar agreement in the event that the Court ruled in auDA's favour following the trial. ...

[187] The unauthorised transfers were made contrary to auDA's *Transfers (Change of Registrar of Record) Policy*, which requires express instructions in

writing for the transfer of a domain name registration from one registrar to another. Further, in the absence of consent from the registrant, a transfer to another registrar contravenes auDA's *Domain Name Password Policy* because it involves the disclosure of a registrant's password to a third party.

64 By ground 6(a) of its grounds of appeal, the appellant complains that his Honour:

... erred in determining that the ... transfers were 'effected ... by' ... the appellant ... when there was no evidence to support such a conclusion (and all of the evidence was to the effect that actions were, in fact, taken by the gaining registrar being Bottle Domains Pty Ltd).

65 This argument cannot be sustained. For one thing, Bottle Domains Pty Ltd and the appellant are members of the Bottle Group. Indeed, it was part of the appellant's case at the trial that they are not only under common ownership and control, but operate with the same personnel. Much more importantly, the transfers could not in any event have taken place without the appellant's approbation - which, in the circumstances of a close relationship between the losing and gaining registrars, amounted to the appellant's active involvement.

66 The next of the appellant's points has superficial merit. It is to the effect that his Honour erred in determining that Australian Style breached auDA's *Transfers (Change of Registrar of Record) Policy*. The fact is (or so the appellant contends) that the policy imposed no obligations on the appellant. It follows that no breach such as his Honour found could have occurred.

67 His Honour, at paragraph [14] of his judgment, noted that, by clause 7 of the registrar agreement, the appellant is required to comply with all of the respondent's published policies, which are to be treated as if incorporated into the agreement. So much is not in dispute. Nor can it be doubted that the effect of the *Transfers (Change of Registrar of Record) Policy* is, as his Honour held:

... clear: a transfer requires the 'gaining registrar' to receive a written request for transfer from the registrant and not to process the transfer until it is affirmed by the registrant.<sup>10</sup>

---

<sup>10</sup> Judgment, [188].

68           The appellant does not suggest that the policy lacked clarity on this point. Rather, it relies on the fact that it (the appellant) was the ‘losing’, while Bottle Domains was the ‘gaining’, registrar. Accordingly, the obligation to refrain from processing transfers until receipt of a written request was on the latter company, not Australian Style.

69           It follows that, if the trial judge found that the appellant’s role was merely that of the ‘losing’ registrar, and as such it was in breach of the requirement that a written request for transfer be received by it before the transfer is processed, he was in error; and ground 6(b) of the grounds of appeal is made out. But as I understand his Honour’s discussion of the point, he held that the appellant was complicit in Bottle Domains’ breach of the policy. Such a finding was in my opinion justified.

70           In any event, another policy of the respondent must be considered. It is raised by ground 6(c). The appellant here contends that his Honour erred in determining that the May 2009 transfers breached the *Domain Name Password Policy*.

71           Two bases are put forward as supporting this contention. The first is expressed in the formulation of the ground as it appears in the notice of appeal. It is there asserted that his Honour erred in determining that ‘the May 2009 transfers breached the *Domain Name Password Policy* ... when there was no evidence of the passwords being disclosed’. The second (as was argued in paragraph 7(b)(i) of the appellant’s written ‘outline of reply submissions’ dated 8 February 2010) is that his Honour was in any event in error in holding that that policy prohibited such disclosure when ‘such a prohibition simply does not appear in [it]’.

72           The particular passage in the judgment to which, in its outline of reply submissions, the appellant takes exception, is to be found in paragraph [187]. His Honour there held that ‘in the absence of consent from the registrant, a transfer to another registrar contravenes auDA’s *Domain Name Password Policy* because it involves the disclosure of a registrant’s password to a third party.’<sup>11</sup>

---

<sup>11</sup>       Ibid, [187].

73

It is true, as the appellant submits, that the policy does not explicitly state that the disclosure of passwords is forbidden. With respect, however, this submission is another example of the point I sought to make in the opening paragraphs of this judgment. The whole tenor of the policy reinforces a precept which should inform every dealing of every registrar worthy of its accreditation: the security of passwords is of paramount importance. If that security is to be maintained, passwords must not be disclosed otherwise than in clearly specified circumstances. Thus, by clause 2.4<sup>12</sup> of the *Domain Name Password Policy*, registrars must when issuing a registrant with a domain name password notify the registrant of ‘the importance of keeping the domain name password secure’. Thereafter, the registrar may not change it without either the consent of the registrant or the permission of auDA.<sup>13</sup> Again, clause 3 of the policy carefully limits the use which a registrar may make of a password. Consistently with this, and most relevantly of all, a registrar ‘must ensure that the domain name password is provided directly to the registrant’<sup>14</sup> unless the latter has given ‘explicit’ permission for its provision to a third party.<sup>15</sup> There can in my opinion be no other conclusion than that the *Domain Name Password Policy* forbids the unauthorised disclosure of passwords.

74

There remains that aspect of ground 6(c) which is raised by the ground as formulated in the notice of appeal: that is, that –

... there was no evidence of the passwords being disclosed but the unchallenged evidence was that the same people worked for the appellant and Bottle Domains Pty Ltd and there was no need for such disclosure upon the transfer.

75

It may be accepted that ‘the same people worked for the appellant and Bottle Domains Pty Ltd’. In my opinion, however, that is not to the point. The proper administration of the domain name system is of such importance that auDA is in the

---

<sup>12</sup> Where first appearing. The *Domain Name Password Policy* contains two paragraphs numbered 2.4.

<sup>13</sup> *Domain Name Password Policy*, clause 2.4 (where appearing for the second time).

<sup>14</sup> *Ibid*, clause 4.2.

<sup>15</sup> *Ibid*, clause 4.4.

circumstances operative here entitled to insist on the letter of its policy being given effect. The appellant and Bottle Domains know how each is structured. Registrants may not. It is their interests which are paramount. They are entitled to refuse to agree to a transfer, and therefore to the disclosure, of their password to a different registrar, even though both new and former registrars may employ the same personnel. After all, each registrar is a separate legal entity, and their financial structures and administrative arrangements may be different. Even supposing that registrants would not be acting rationally were they to object to a disclosure of their passwords in the circumstances which obtain here, it is their passwords and their interests which are being transferred or affected, and they must have the right – denied to them by the appellant – to veto any proposed change. It is pertinent in this context to note that, in his affidavit seeking injunctive relief, Mr Bolton swore that Australian Style was ‘finding it very difficult to convince [registrants] to transfer the registration of their domain names to another one of Australian Style [Bottle] Group’s registrars’.

76           For this reason, ground 6(c) also fails.

77           Ground 7 is that the trial judge ‘erred in failing to determine that any breach of any policy created by the May 2009 transfers was a breach that was capable of being (and was) remedied’. And it is true that, in the sense and to the extent that transfers can be reversed, the capacity for remedial action exists.

78           auDA, however, relied upon the May 2009 transfers principally because (as auDA asserted and, for the reasons given at paragraphs [191] and [192] of his judgment, his Honour found) they constituted a breach by Australian Style of ‘its obligation to act in good faith in its dealings with auDA’.<sup>16</sup> In my opinion, his Honour was fully justified in so finding.

79           One consideration in particular seems to me to be conclusive. In my opinion, the appellant acted in bad faith following its success in obtaining injunctive relief.

---

<sup>16</sup> Judgment, [192].

I return to this issue when considering ground 8 of the grounds of appeal. For the present, I observe that, when making its application to the Court, Australian Style submitted that the balance of convenience favoured the granting of the injunctions because its business would otherwise be destroyed, jobs would be lost, resellers would be put to enormous difficulty, and (most relevant in this context) if it were ultimately successful in setting aside the notice of termination, registrants would have gone to the trouble of changing registrars for no good reason.

80           It was wholly inconsistent with this submission to then effect the very change which the submission characterised as undesirable. In my opinion, such inconsistency amounted to an act of bad faith.

81           The next question is whether this is a failing which can be remedied. I agree with his Honour that it cannot. Once committed, an act of bad faith cannot be undone. It remains an act of bad faith no matter what steps might be taken to neutralise its effects. Those steps might be wholly successful, just as a thief might make reparations for his or her crime by returning the stolen goods in the condition in which they were when misappropriated. In that sense, a remedy might exist. But the fact of the theft remains. And the thief remains guilty of it. In the context of the proper administration of the .au domain name system as a public resource for the public benefit, the same reasoning must apply. auDA as the administrator of the system must, in my opinion, therefore retain the right to treat an act of bad faith as a breach of clause 14.1.1 of the registrar agreement, and therefore as an event of default under clause 23.1.4 of that agreement, even if the damage caused by that act can be repaired. And that right should remain no matter what corrective action is taken, and notwithstanding that in one sense that action is 'remedial'. Of course, it does not follow that an act of bad faith will inevitably result in suspension or termination pursuant to clause 4; that will remain a matter within the discretion of auDA. Its discretion must itself be exercised in the light of (among other things) any corrective or 'remedial' steps, as well as auDA's own obligation to act in good faith.

82           For these reasons, ground 7 of the grounds of appeal cannot be upheld.

83 This conclusion also applies to ground 8, which is that his Honour erred in determining that, in the circumstances specified, the May 2009 transfers constituted a breach of the appellant's obligation of good faith in its dealings with the respondent.

84 The first of these circumstances is that his Honour wrongly (as the appellant would have it) 'assumed ... that the May 2009 transfers were effected administratively by the appellant'. The answer is that, as discussed in relation to ground 6(a), Bottle Domains may have been the active party, but it could not have proceeded without Australian Style's approbation.

85 The second of the circumstances alleged to having been applicable in the supposed error of the trial judge is that 'the interlocutory injunctions ... did not impose any restrictions on the appellant'. Accordingly, the appellant took the view that it could participate in the transfer of 95% of its registrants to another member of the Bottle Group, and could do so without any qualms about the effect of the orders of the Court. As for the wishes of its registrants, they for other reasons could also be put aside.

86 But, as it seemed to the trial judge, there were problems with this view. First, the injunctions were intended to preserve the status quo. The transfers not only had the opposite effect; they also (and this was the second problem) interfered with the interests of the appellant's registrants. Most importantly, perhaps, they demonstrated that the appellant had not then, and may not have yet, perceived that the necessity for good faith (on the part of all registrars on the one hand and auDA on the other) arises not merely - or even principally - out of the contractual relationship between parties engaged in a commercial enterprise; after all, the relationship is not entirely commercial: although each registrar operates a business, auDA is not a profit-making body. Rather, good faith is an essential element in the dealings between registrars and auDA because the .au domain name system is a public resource which must be administered in the public interest. A lack of good faith in dealings between a registrar and its registrants may, therefore, also qualify as a lack of good faith as between that registrar and auDA. In my opinion, the

involvement of Australian Style in the post-injunction transfers in fact so qualified. The circumstance that the appellant has in this way demonstrated that it has an inadequate concept of the notions of good and bad faith is also, it seems to me, reason enough to question whether it is worthy of accreditation as a registrar.

87 The third of the 'circumstances' in which his Honour is said to have erred in determining that the May 2009 transfers constituted a breach of the obligation of good faith is set out in ground 8(c) of the grounds of appeal, and is that:

(c) contrary to the finding of his Honour (at paragraph [192]), the purpose of the May 2009 transfers was not to defeat the efficacy of the notice of termination ... in circumstances where:

- (i) the purpose of such notice was to terminate the accreditation and the registrar agreement *of the appellant*<sup>17</sup> (and not to terminate the accreditation and the registrar agreements of all registrars in the same group of companies as the appellant as his Honour expressly found at paragraph [189]), and the effect of the May 2009 transfers was to transfer the registration of domain names away from the appellant; and
- (ii) at all times both before and after the May 2009 transfers, registrants retained the ability to make a choice as [to] which registrar they wished to use and the respondent did not have any interest in having the registration of the domain names the subject of the May 2009 transfers remain registered in its name as it was an interim registrar only until registrants chose another registrar (paragraph [9])

88 The passage quoted contains a reference to paragraph [189], and a reference to paragraph [9], of his Honour's judgment. In paragraph [189], the trial judge notes the evidence about Mr Disspain's separate treatment of each registrar, and the resultant decision by auDa to terminate 'Australian Style's registrar agreement only and, notwithstanding the conduct of Mr Bolton, [to take] no action against the other three registrars in the Australian Style [Bottle] Group' (one of which is Bottle Domains). The reference to paragraph [9] of the judgment was doubtless inserted because the judge there includes, in his enumeration of the elements of the .au domain name system, the right of registrants to choose to transfer to another registrar.

---

<sup>17</sup> Emphasis as in the original.

89           In my opinion, acceptance of ground 8(c) of the grounds of appeal would involve a preference for form over substance. It is true that auDA intended to terminate the appellant's registrar agreement, but did not intend to interfere with those of other members of the Bottle Group. It is also true that the effect of the May 2009 transfers was in one sense consistent with that purpose, because it was designed to replace the appellant as the registrar of those registrants then on its books, and substitute Bottle Domains in its stead. It is, in addition, true that the respondent was an interim (default) registrar only, and that registrants could always choose to go elsewhere. Overriding all this, however, was the appellant's ultimate purpose.

90           In my opinion, his Honour was correct in finding that it was Australian Style's desire (as the grounds of appeal record) 'to defeat the efficacy of the notice of termination' should auDA ultimately succeed in this litigation. If at that point Australian Style had no registrants, because they had all been transferred to Bottle Domains, the termination of its registrar agreement would have no effect on the business of the Bottle Group. auDA would not be in a position to resume its role as default registrar because there would be no domain names, and no registrants, for which auDA could become responsible. Accordingly, there would be no domain names, and no registrants, for whom auDA could act until they found a new and permanent registrar. The group would have retained the appellant's registrants, albeit with another group member, and would therefore have retained their business. The fact that in theory the registrants could go elsewhere would in practice be irrelevant, because in practice Newton's law applies. People, like things, tend to remain where they are. In other words, if things worked out as planned, the Bottle Group would not suffer - or not suffer much - no matter what might be the ultimate fate of Australian Style.

91           But that result would not accord with the due administration of the .au domain name system as a public resource. The interests of the public, insofar as the public was and is represented by Australian Style's registrants, would take second

place. His Honour found (at paragraph [185] of his judgment) that none of them were consulted in advance of the unauthorised transfers (and no prior notification was given to the Court or to auDA). So the registrants would without notice find themselves on the books of Bottle Domains and off the books of Australian Style: a circumstance which the respondent's policies were designed to forestall. Of course, they could move elsewhere; but whereas when under the umbrella of auDA following the respondent's ultimate success in this litigation (should that be the result) they would actively select a new registrar which might well not be a member of the Bottle Group, if the plan behind the May 2009 transfers succeeded, they would be Bottle Domains' registrants, with good prospects of their retention by that entity.

92 His Honour found, and I agree, that this account of the manoeuvrings of the appellant evidenced a lack of good faith. Ground 8 of the grounds of appeal therefore fails.

93 Allegations that the appellant did not act in good faith also form the basis of the contentions which, should the appeal otherwise succeed, the respondent would wish to advance as justification for its termination of the registrar agreement. One of these concerns the post-injunction transfers considered above. As set out in auDA's notice of contention, however, the first assertion of bad faith arises out of the negotiations between the respondent and the appellant after the disclosure of the 2009 security breach. The respondent required the appellant to disseminate by email to its registrants certain information about the breach. A draft, which referred registrants to the need for vigilance, and recommended careful monitoring of 'your domains, your account and your credit card transactions' was prepared by the appellant. The respondent's agreement to that draft was confirmed by email sent by Mr Disspain to the appellant at 11.29am on Monday 9 February 2009. At the same time, Mr Disspain told the appellant that the agreed email must be forwarded to all registrants within the next two hours. At 12.30pm, Mr Bolton informed the respondent that Australian Style would 'send our notice in the next hour'.<sup>18</sup>

---

<sup>18</sup> Judgment, [41].

94           That did not happen. Instead, at 1.34pm Mr Bolton sent an email to Mr Disspain. This referred to 'a summary document' which Mr Bolton had prepared 'outlining our actions as a result of this event.' That document, however, included an amended draft email to which, in his covering correspondence, Mr Bolton made no reference. The agreed version had included a passage to which I have already alluded, but which read in full:

          During this time, we recommend that you remain vigilant, and carefully monitor your domains, your account and your credit card transactions. Please contact us immediately if you are aware of anything out of the ordinary.

The amended version omitted any reference to credit cards.

95           Mr Disspain did not read the 'summary document' immediately. Indeed, as his Honour recounted the evidence:

          To [Mr Disspain's] recollection, he first read [it] at a later time, once it became apparent that Mr Bolton was alleging that the summary document contained an amended version of the agreed email.

96           Before Mr Disspain appreciated this, however, he became impatient because the appellant had not dispatched anything to its registrants. At 3.30pm, he communicated his displeasure to Australian Style, and notified the appellant of his intention to send, 'within the next hour' an auDA email to Australian Style's registrants. Mr Bolton quickly responded:

          Hi Chris,

          I don't think that's necessary. Customers are not presently at risk, and we are working as quickly as possible to get this done. ... I don't feel auDA taking matters into their own hands is in the best interests of this issue.

97           It was not until 8.22 that Mr Bolton told Mr Disspain that emails had been sent to Australian Style's registrants. But they were not in the agreed form. They did not even conform to the 'amended' version, the transmission of which had been concealed by the deceptive wording of the 'summary document'. They constituted a different version again, omitting altogether the recommendation that registrants remain vigilant and monitor their domains, accounts and credit card transactions. As his Honour also found:

There were other changes which had the obvious intention of downplaying the seriousness of the security breach and seeking to reassure registrants that it was unlikely their private information had been accessed.<sup>19</sup>

98 Mr Bolton said that he did not intend to send this email. It went out by mistake. He had made a 'cut and paste error'.

99 The trial judge did not believe this. His Honour found that the defective email was 'the result of a deliberate decision by Mr Bolton.'<sup>20</sup> The judge also found that:

the inclusion of the amended email in the summary document ... without indicating that an amended version of the agreed email was being proposed, was sharp practice ... The proposed amendment should have been brought directly to Mr Disspain's attention. Even if Mr Bolton had then sent an amended email, and not the defective email, this alone was in my view conduct in breach of the express obligation upon Australian Style under clause 14.1.1 of the registrar agreement to act in good faith in its dealings with auDA.

100 These were findings to which in my opinion his Honour was fully entitled to come. I also agree with his Honour that the lack of good faith demonstrated by the appellant in its dealings with auDa over the post 2009-breach emails was such as to justify the respondent's decision to terminate the appellant's registrar agreement. That being so, it follows that ground 1.1 of the respondent's notice of contention must succeed.

101 The notice of contention pleads two other bases for termination on the ground of bad faith. One rests on his Honour's finding that, contrary to the evidence of Mr Bolton, the appellant failed to test, or to test adequately, the security patch provided to it by Aust Domains after the 2007 breach. The second is founded on Mr Disspain's belief, which his Honour at paragraph [172] of his judgment held to be reasonable, that by his post 2007 security breach behaviour Mr Bolton had demonstrated a lack of appreciation of the significance of a security breach.

102 Neither of these matters was, of itself, held by his Honour to provide a proper

---

<sup>19</sup> Judgment, [55].

<sup>20</sup> Ibid, [141].

basis for the termination of the appellant's registrar agreement. They were simply placed in the total mix. Given the findings to which I have already come, there is no need to consider whether, either alone or in combination, they would be properly considered as decisive.

103           Nor is there need to consider a matter raised for the first time on the appeal: that clause 4.2 of the registrar agreement is void because it constitutes an ouster of the Court's jurisdiction. That clause provides that 'auDA may suspend or terminate the registrar's accreditation if auDA considers that an event of default has occurred in respect of the registrar.' The point, however, only arises if leave to argue it is given and - more importantly - the Court is of the view that the trial judge erred in holding that the respondent was entitled to terminate the registrar agreement. I am not of that view.

104           In my opinion, for the reasons given above, his Honour correctly decided the points at issue in grounds 6-8 of the grounds of appeal, and correctly dealt with those raised by the notice of contention. For all the reasons set out in this judgment, the appeal must be dismissed.

---