

consumerwatch



76	ConsumerWatch
78	Who's holding your data?
79	Searching for help
80	Prints harming
82	Supplier profile: Toshiba
86	Technology in action

If you're thinking of upgrading rather than buying a whole new PC, check first that your warranty won't be invalidated. Meanwhile one reader discovers patience is a virtue when you're waiting for BT to activate your phoneline for ADSL



The first-time PC buyer market is shrinking all the time. Manufacturers are up against a gloomy economic outlook as well as an increase in DIY upgrades. Customers are buying parts as they need them rather than splashing out on whole systems.

As well as proving cheaper than shelling out for the latest PC every couple of years, users can personalise their systems from the casing to the components to suit their needs. And if you don't have the technical know-how to install the necessary parts, it's still cost-effective to have them fitted by an expert.

But there is a down side. Such alterations will probably have an impact on the PC's warranty. Some manufacturers are more lenient than others, choosing not to void the warranty completely but to limit cover to only the original parts. However, there is always the danger a warranty will be invalidated by the smallest change from the original specification and leave the customer without any technical support.

Be aware that any damage caused to existing components by new parts will often not be covered. Instead only the

original system will be insured under the terms of the warranty, making upgrades a risky business.

Minimising risk

Recognising the upgrade trend, computer maker Time has included an upgrade option in its Total Care Cover Gold plan in a bid to encourage users to upgrade using

"Our terms and conditions clearly explain the parameters of the warranty, but always contact the PC manufacturer for clarification before you carry out any upgrades."

Jag Mann, product manager, Multivision

its parts. Rival manufacturers Systemax and Multivision have also adopted the same line of thinking, extending warranties to cover their own parts but not third-party components.

"Our terms and conditions clearly explain the parameters of the warranty, but it's always wise to contact the PC manufacturer for clarification before you carry out any upgrades. Once you've done it, it's too late," advises Multivision's Jag Mann. Our advice? Upgrade with third-party components at your own risk.

Internet confusion

Reader Graham Muir contacted us about his on-going problem with ISP Gio Internet. He signed up to its broadband package, due primarily to its affordable £18.99 monthly charge, but unfortunately the supplied username and password did not seem to work.

He returned his modem to Gio only to be told it was in full working order and that there was no problem with the logon details supplied. After another unsuccessful attempt at accessing his account, Graham was advised to call Gio's premium rate phoneline.

Despite leaving a message on the 60p-per-minute line, his call was never returned. Rather than continue paying for a service he couldn't use, Graham tried to cancel his subscription but was told he could only do so after the first two months and even then he would be required to give 30 days notice.

Gio Internet told us there had been some delay in BT's activation procedure, but that Graham's line is now working. A spokesman for Gio Internet said that BT carries out tests through its servers and the ADSL pathway in each area before its customers can access their accounts. This usually takes about four weeks but in Graham's case there were inexplicable delays. The frustration for customers is that BT will not confirm whether a line has been activated.

The ISP, meanwhile, can do little else but wait for BT's signal that the line is

working. Gio has since apologised to Graham, promising to give him two months free service on top of the two months he has already shelled out for. A happy ending in what continues to be a frustrating situation for those connecting to BT's ADSL networks.

BT Connect gets blacklisted

There are hundreds of organisations which run blacklists – rollcalls featuring negligent companies. Many lists focus on the ever-growing problem of spam, targeting businesses that send a large proportion of unsolicited emails over their networks.

For instance, Distributed Server Boycott List (www.dsbl.org) blacklisted BT Connect, which is part of BT Openworld, for running an open-relay server which could be easily exploited by non-BT Connect customers to launder junk email. Thus spammers are able to slip through filters to send out thousands of unwanted messages.

However, the blacklisting caused problems for reader Martin Holcombe who found he couldn't send emails from his BT Connect business account, meaning he was paying for a service he couldn't access. As we went to press, he still couldn't use it.

BT emailed Martin assuring him it did not run an open-relay server. Instead it stated that "because of the way our servers work within a specific range of IP addresses, some mail will [not] go through

PC Advisor personal data privacy campaign

Have you ever been sold a PC that had someone else's information on? Or has a PC you returned to a company been resold without being properly wiped? If either of these things have happened to you, we want to hear from you. If you find a previous customer's data on a PC purchased from the Dixons Stores Group don't forget to email Simon Turner the managing director at simon.turner@dixons.co.uk.



Email us at pcadvisor_consumerwatch@idg.com and we'll take it from there

for [some] domains, but it is still not open-relay", which did nothing to help. And the telco offered little hope of correcting the problem: "The position as it stands is that we cannot change the way that our servers work with regards to our customers. We therefore cannot at this moment in time clarify when this can be rectified."

We contacted Distributed Server Boycott List which assured us BT was running an open-relay server. "BT Connect's outgoing servers are wide-open single-stage relays," said a DSBL spokesman. "Its servers have [previously] been removed from DSBL, but they didn't fix the [open-relay] problem so were listed again. It's useless to remove a host from DSBL without fixing the

problem that caused the original listing." A second expert at DSBL agreed this was BT's responsibility.

"BT Connect's mail servers are open-relay plain and simple. Evidence for all listings is provided on DSBL's website. I fail to see how they can claim not to have a problem when the evidence is clear to see," he added. BT is adamant it does not use open-relay servers: "If we did, millions of customers would have been affected," said a company spokeswoman.

To make matters worse, Martin then received a rather rude email from BT's helpdesk asking him not to copy in *PC Advisor* on any correspondence with them. It advised "not to construe information that was provided involuntarily and without malice which was provided on a confidential basis".

At *PC Advisor* we have never come across such a problem with any other service provider. BT Openworld's press officer assured us this email problem would be dealt with. "Obviously more training is needed here and we can only apologise," said a spokesman. BT is currently in talks with DSBL to "fulfil certain criteria" so that it can be removed from the blacklist.

The company will be contacting its customers to advise them of server changes which may affect service. The process should be complete, according to BT, within the next fortnight... Here's hoping. Watch this space. ■

Extended warranties: state of play

The Competition Commission's letter to retailers detailing possible remedies to the debate over extended warranties (see News, page 18) could mean that shops will have to provide information on alternative warranty providers. The CC recommends sales staff show customers price comparison tables for different warranty deals offered by other companies.

But Rectra (the Radio, Electrical and Television Retailers Association) has complained that such a requirement would be uncompetitive, especially to smaller firms. Correlating such information is a time-consuming task, argues Rectra, and it would be simply

unfair to force retailers to advertise competitors' services at a potential financial loss to themselves.

But providing consumers with such information would allow them to make a more informed decision about one of the most expensive purchases there is after buying a home or car.

Retailers were given just over two weeks to respond to the CC's recommendations; the consultation period ends 6 June. Dealers have chosen not to speak to the press until the debate is complete – no doubt a ploy to allow them to claim victory when the CC announces its final decision on 1 July.



Got a problem with a vendor? Log on to the ConsumerWatch forum for instant help and advice www.pcadvisor.co.uk/consumerwatch

who's holding your data?

More than a quarter of *PC Advisor* readers appear to favour Home Office proposals to force ISPs to retain all details of customer internet activity. Guy Dixon asks them to think again

An astonishing 27.2 percent of *PC Advisor* readers believe the Home Office has every right to access data on the internet activity of all UK consumers in the interests of national security. That's according to a recent poll on the *PC Advisor* website.

We have to confess, we were somewhat taken aback by the sheer number of readers who appear happy to hand over their virtual privacy rights in one fell swoop. The very nature of a democratic society involves striking a balance between respect for the privacy of a member of the public and ensuring that same citizen is protected from crime.

But we believe that the Home Office's intention to retain data about and snoop on the internet activity of everyone in the UK is likely to upset that balance as well as place an unfair burden on this country's ISPs.

Code of conduct

In the absence of the emergence of a code of practice – regarded as unlikely by almost all quarters – under the Anti-Terrorism, Crime and Security Act (2001), the Home Secretary is likely to make it obligatory for service providers to store logs of all customers' online activities for at least a year.

The justification is they may one day need such data for subsequent investigations into serious crime or terrorism. Data will include records of all websites visited by a customer, along with all emails sent and received. Instant messaging is not covered (for now).

It's not just the usual privacy liberties brigade, such as Privacy International and the Foundation for Information Policy Research, that are screaming blue murder. Ipsa (the Internet Service Providers Association), has labelled any such blanket policy as impossibly costly and unworkable. It points out it would take over 360,000 CDs to store just one year of customer data.

Let's be extremely conservative and say a third of the UK population – around 20 million – regularly use the internet.

PC Advisor poll

In the interests of national security, the Home Office has every right to access data on the internet activity of all UK consumers:

Agree
 (27.2%)

Disagree
 (63.8%)

Data retention requires ISPs to keep logs on all customers. The Home Office has threatened to make this obligatory

conducted June 03, 3,087 respondents

That means in the course of a year the UK's ISPs would amass the equivalent of 7,200 billion CDs. Take into account a steady increase in internet users, sites visited, emails sent and received, and it doesn't take a genius to see that we'll soon be drowning in a sea of retained data.

What's more, the sheer cost of adhering to these laws – independent estimates put this at well over £100m – could put many service providers out of business. Most are already offering broadband services with wafer-thin profit margins; such enforced co-operation could bankrupt them.

Drastic measures

It's also not clear that the fight against terrorism and serious crime can't be won without such drastic measures. In the US – where respect for individual privacy is arguably greater – this does not happen. The FBI prefers a more targeted scheme using so-called data preservation. This is where service providers hold data on specified individuals at the request of the authorities.

The extent of government snooping is growing and it needs to be watched. The Home Office only recently abandoned plans to give a wide range of minor authorities – even local town halls – the right to request information on your surfing habits. Only an uproar from civil liberties groups forced them to back down.

In short, we're asking a quarter of poll respondents to think again. ■



It's a fact

- We pay to be snooped on **Data retention is likely to cost in excess of £100m per year and will be funded by tax payers and UK ISPs.**
- Legally, the police can request information on an individual **Data preservation requires service providers to retain data on specific individuals at the request of the police. This is the approach taken by US authorities and is the option favoured by UK ISPs.**
- Logs may be kept on everyone by law **Data retention requires ISPs to keep logs on all customers. The Home Office has threatened to make this obligatory.**
- Communication is key **The two key pieces of legislation are Anti-Terrorism, Crime and Security Act (2001) and the Regulation of Investigatory Powers Act (2000). These acts cover communications data – the logging of information held by ISPs, phone companies and mobile operators.**

searching for help

The PC Advisor ConsumerWatch online forum now has more than 60,000 postings primed with comments about customer service and consumer rights. Guy Dixon takes it for a spin

As regular readers will know, most of the stories we deal with in this section arise from issues aired in the online ConsumerWatch forum at www.pcadvisor.co.uk/consumerwatch.

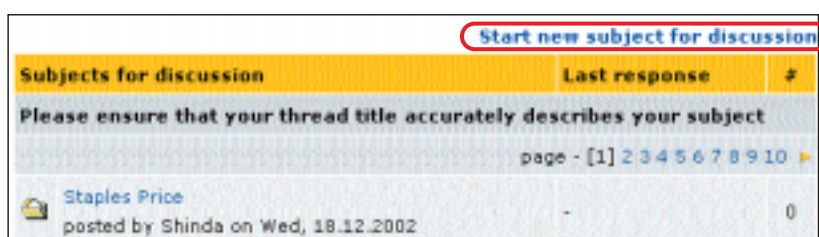
While we're more than happy to receive emails and letters from aggrieved readers, and do everything we can to help, a trip to the ConsumerWatch forum is more likely to result in a rapid and useful response.

Help yourself

We have a live walk-in consumer affairs clinic, which will automatically send you an email the moment that someone responds to your query. The ConsumerWatch forum is constantly checked by editorial members of staff, our forum editor, IT consultant Peter Thomas and the UK computer industry's leading vendors including Dell, Evesham, Mesh, Multivision, Time and many others.

Last, but not least, our online forum is manned by dozens of knowledgeable website regulars, ready and willing to lend a hand. Whether it's delivery problems, faulty goods or poor service you're experiencing, the ConsumerWatch forum is here to help. ■

Live clinic



1 To make a posting click on 'Start new subject for discussion'

2 Enter a description of your problem next to 'Title' – for example, 'Monitor keeps flickering: just three weeks old'. Enter a more detailed description in the dialog box next to 'Message' and click 'Begin new subject for discussion'



3 The posting appears at the top of the forum threads. When someone responds to your thread you're notified by email. Once your problem is successfully resolved click the resolved checkbox. Visitors can now sift answered queries from unanswered ones

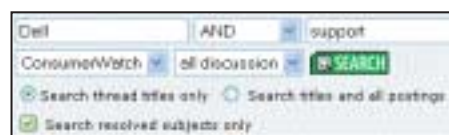
Search facilities

Visitors not only use the ConsumerWatch forum for live help, but also to get background information using its impressive search facilities. There are over 60,000 messages sitting in the database, so you can check on the reputation of a manufacturer or retailer.

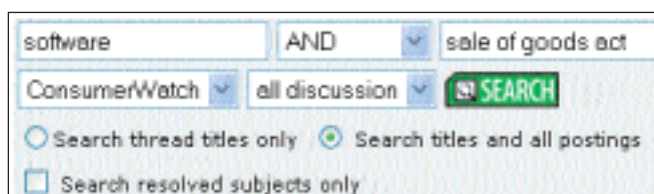
Alternatively, you can search for consumer rights issues under a specific term.



1 Search using Boolean logic terms in your search title, such as 'and', 'or' and 'and not'



2 There's different levels of targeting to choose from – for example, the most highly targeted is a request to search on resolved subjects only or thread titles only



3 Alternatively, search for obscure topics on a much broader level by opting for 'Search titles and all postings', such as a search on 'software' and 'Sale of Goods Act'