He estimates that the majority of current queries already search enough computers to return useful results.

Crick counters, however, that "many people who give that argument don't understand the possible efficiency benefits that come out of using distributed hash tables." Unlike earlier attempts, he says, "NEOnet provides better results for all searches using less traffic" than the existing peer-to-peer search technology.

Bildson's opinion matters because—along with several other ventures—LimeWire and Streamcast share users to a degree. They are all using Gnutella, an open-source protocol that provides basic peer-to-peer file-sharing services. Each vendor builds additional features, such as NEOnet, on top of the basic protocol, but tries

Streamcast hopes, through NEOnet, to help users find not just pop music but also needed information, software, and services

to make sure its software stays on speaking terms with the other Gnutella programs. The situation is somewhat analogous to that of different e-mail software vendors who have to maintain interoperability.

But sometimes spats flare up. Before NEOnet's incorporation into the Morpheus software, LimeWire "took steps at the beginning of the year to cut [Streamcast] off the network," remembers Bildson, because computers running Morpheus "weren't responding to searches and were completely leeching off the network."

In the end, Streamcast and LimeWire worked together to resolve the technical issues involved, but Streamcast's CEO Michael Weiss is stung by suggestions that his company isn't contributing its fair share to the success of the Gnutella network. He points to Streamcast's successful legal defense of the network against the Recording Industry Association of America (RIAA), Washington, D.C. "If it wasn't for Morpheus and our litigation, most of these other companies would be sued out of existence," says Weiss.

To the RIAA's chagrin, in August the courts ruled that peer-to-peer software vendors can't be held liable when users of their software illegally swap copyrighted material. There's no liability, the courts said, because the decentralized nature of the networks means that vendors have no control over what users do and because the software can also be used to distribute material legally.

Legal distribution is the future of peer-to-peer, as Weiss sees it, and this vision is why NEOnet is so important to Streamcast's strategy. It seeks, through NEOnet's improved ability, to find files other than music or the pinup du jour, to get users to accept Streamcast's peer-to-peer network as a reliable place to find legitimate information, entertainment, or software, much as the Web is used today. But NEOnet also offers the advantage that a peer-to-peer network can help share the load (and the bandwidth costs) currently associated with hosting such content on the Web.

Weiss calls this ability to find rare content "Googlizing peer-to-peer," and to get the ball rolling, Streamcast is working with Creative Commons, a San Francisco–based nonprofit that encourages duplication-friendly copyright licenses. The companies plan to set up a mechanism that allows easy searches through Morpheus for material licensed for legal peer-to-peer trading.

—STEPHEN CASS

Editor's note: Francis Crick's sister, Camberley Crick, is an editorial intern at *IEEE Spectrum*. She was excluded from the reporting and editing of this article.

WHOSE FAULT? Increasingly, when there's a wreck like this, information on the crash can be recovered from a "black box."

Black Boxes Get Green Light

But crash data recorders in cars raise privacy concerns

Car buyers are faced with a dizzying array of options. But there is one important added feature not included on the window sticker or in any options package: a box of electronics the size of a pack of cigarettes that is a less refined version of the so-called black box carried in aircraft, which becomes the focus of attention after a plane crash. According to the U.S. National Highway Traffic Safety Administration (NHTSA), more than 65 percent of 2004 model year cars sold in the United States, the world's largest passenger car market, have some sort of event data recorder. Yet the average driver has no idea that in the event of a crash, a record of how the car was being driven in the moments just before impact has been created and is stored onboard [see photo, "Whose Fault?"].

Often, people learn of the box's existence only when a lawyer introduces the data it contains in court to back up their version of events. In one well-publicized recent case, a Florida man was convicted in 2003 of two counts of manslaughter and two counts of vehicular homicide when the event data recorder in his 2002 Pontiac Trans Am showed that he was traveling at 114 miles per hour (184 kilometers per hour) in an area where the posted speed limit was 30 mph (48 km/h) when he collided with another car, killing two teenage girls.

AS MANY AS 40 MILLION CARS on U.S. roads now carry event data recorders, it's estimated. Even so, their installation in cars did not become much of a public issue until August, when the U.S. National Transportation Safety Board (NTSB) recommended that they be required in all new passenger vehicles. Then, on 23 September, the IEEE announced that one of its committees had created the world's first technical standard for the devices.

D. ROSE/MASTERFILE

At present, the recorders' capabilities vary widely. The IEEE effort aims to make it possible to gather the same pieces of information from any crash. The IEEE 1616 standard creates a baseline for what data—say, velocity, engine revolutions per minute, throttle position, use of brakes or seat belts—recorders will store and for how tamper-proof and crash-proof the boxes must be. "The more accurate the data we gather on highway crashes, the better chance we have to reduce their devastating effects," says Jim Hall, a former NTSB head and cochair of the working group that developed the standard.

There is no disputing that there are legitimate benefits to be realized from the broad adoption of automotive black boxes. Thomas M. Kowalick, the other cochair of the IEEE 1616 working group, told *IEEE Spectrum*, "There has been a stalemate in safety—still no real solution to reduce the number of highway fatalities below about 43 000." Worldwide, of course, the number is much higher.

Today's event data recorders are descended from General Motors Corp.'s Sensing and Diagnostic Module, which was created in the 1970s simply to differentiate between events like stopping short when a child runs into the street and the violent change in velocity that occurs in a collision. The module ensured that a car's air bag inflated only when necessary. The latest generation of event data recorders in wide production is capable of storing 5 seconds of data—continuously updated in first-in, first-out fashion until an air bag is deployed. At that instant, an indelible snapshot of the previous five seconds is stored in the module's read-only memory.

Even this limited data-gathering capability may evoke Orwellian anxieties, but privacy advocates are more concerned about the much more extensive capabilities just up the road. Kowalick, author of *Fatal Exit*, a just-published IEEE–Wiley book examining the ongoing automotive black box debate, shares those concerns. "The worst fears about [event data recorders] are not about what's in cars now, but how [they] could be used in the future," he says. For example, NHTSA has proposed a national crash database, with entries culled from ubiquitous data recorders.

In 1994, when General Motors, in Detroit, put the devices in its cars, it claimed that recovered data were strictly for its internal use. Its engineers, the company said, would be able to design safer cars. As proof, it pointed to the modules' role in pinpointing a flaw that was causing air bags in some of its cars to inflate accidentally. But in the years since, GM has approved the manufacture of machines that allow third parties—such as law enforcement agencies, emergency responders, insurance companies, and people who specialize in accident reconstruction—to download a data recorder's contents. The company that makes the US $2500 readers, Santa Barbara, Calif.–based Vetronix Corp., says it has sold more than 1000 of them so far.

MORE PEOPLE are getting more information about drivers than ever before, as the ability to monitor a vehicle's performance is being combined with wireless communications technologies. Cars are already wirelessly transmitting crash data to local emergency response centers. Soon your car will keep an up-to-the-minute record of your driving from the instant you start it up, and be able to transmit data—including where you went, the route you took, and how fast you drove—over wireless networks.

Given those growing capabilities, it's no surprise that the commercialization of crash data is just around the corner. Insurance companies are beginning to run trial programs offering incentives to drivers who agree to have modules installed that track how often they drive, how they behave behind the wheel, and where they park.

In August, Progressive Corp., an insurance company in Mayfield Village, Ohio, introduced a voluntary program called TripSense for its customers in Minnesota. Those willing to connect a free TripSensor module to their car's diagnostic system get a discount. When it's time to renew the insurance policy, they can download the data stored in the module to their home computers. If the results make the drivers eligible for more discounts, they can send the data to the company.

Though Progressive insists that the program is optional and that data its customers share will never cause their premiums to increase, consumer advocates worry that as insurers become accustomed to being able to ferret out reckless drivers and those out to commit insurance fraud, people unwilling to be monitored in this fashion will find it difficult to get insurance coverage.

—WILLIE D. JONES