BERLIN -- When the Austrian government passed a law this year allowing police to install closed-circuit surveillance cameras in public spaces without a court order, the Austrian civil liberties group Quintessenz vowed to watch the watchers.

Members of the organization worked out a way to intercept the camera images with an inexpensive, 1-GHz satellite receiver. The signal could then be descrambled using hardware designed to enhance copy-protected video as it's transferred from DVD to VHS tape.

The Quintessenz activists then began figuring out how to blind the cameras with balloons, lasers and infrared devices.

And, just for fun, the group created an anonymous surveillance system that uses face-recognition software to place a black stripe over the eyes of people whose images are recorded.

Quintessenz members Adrian Dabrowski and Martin Slunksy presented their video-surveillance research at the 22nd annual Chaos Communication Congress here this week. Five hundred hackers jammed into a meeting room for a presentation that fit nicely into CCC's 2005 theme of "private investigations."

Slunksy pointed out that searching for special strings in Google, such as *axis-cgi/*, will return links that access internet-connected cameras around the world. Quintessenz developers entered these Google results into a database, analyzed the IP addresses and set up a website that gives users the ability to search by country or topic -- and then rate the cameras.

"You can use this to see if you are being watched in your daily life," said Dabrowski.

The conference, hosted by Germany's Chaos Computer Club, featured many discussions on data interception and pushing back the unprecedented onslaught of surveillance technologies.

Even the Dutch, once known as hacker-friendly, politically progressive Europeans, are now fearful and demanding more cameras on their streets, said Rop Gonggrijp, founder of Dutch ISP Xs4All.

Gonggrijp says the Dutch chief of police has announced the intention to store large amounts of surveillance data and mine it to determine who to pressure and question. "People are screaming for more control," said Gonggrijp.

Dutch journalist Brenno de Winter warned that the European Parliament's support for data retention doesn't ensure security, and makes citizens vulnerable to automated traffic analysis of who communicates with whom through phone calls and internet connections. "What we have seen is a system that fails because we miss out on too much information,

and even if we have all that information, it doesn't give us the right information and it is easy to circumvent," said de Winter.

CCC member and security researcher Frank Rieger said hackers should provide secure communications for political and social movements and encourage the widespread use of anonymity technologies. He said people on the other side of the camera need to be laughed at and shamed.

"It must not be cool anymore to have access to this data," said Rieger, who argued that Western societies are becoming democratically legitimized police states ruled by an unaccountable elite. "We have enough technical knowledge to turn this around; let's expose them in public, publish everything we know about them and let them know how it feels to be under surveillance."

The four-day Chaos Computer Congress is meeting near Alexanderplatz in the former East Berlin, where more than a half-million people rallied for political reform five days before the fall of the Berlin Wall.

In his keynote address, Joichi Ito, general manager of international operations for Technorati, warned that the internet could itself become a walled-in network controlled by the International Telecommunication Union, Microsoft and telecommunications companies.

Ito said these restrictions would stifle free speech and the ability to question authority without retribution. "An open network is more important for democracy than the right to bear arms and the right to vote," said Ito. "Voice is more important than votes."