

Democracy and Technology

Chris Morris, *Chester, UK*

Kai A. Olsen, *University of Bergen and Molde College, Norway*



Digital technology has profound social implications that bring with them ethical responsibilities for computing professionals.

An essay by Kai A. Olsen that was published in this column in April 2010 ("Computing a Better World," pp. 96, 94-95) generated a comment from David Anderson that was included in the August 2010 Letters column along with a response from Olsen. That exchange prompted a further comment from Chris Morris that is presented here under the heading "Thrust," followed by Olsen's response, under the heading "Riposte."

THRUST

Here in the UK, everyone arrested for a crime must surrender a DNA sample, with approximately 4 million samples having been recorded. By policy, partial matches are only used when investigating serious crimes.

An example of the use of this kind of evidence occurred in 2009, when Paul Hutchinson was arrested for a rape and murder committed in 1983. Initially, the police had analyzed DNA found in samples from the crime scene, but no database record matched the samples. However, 26 years later, a partial match was found when a DNA sample was obtained from Hutchinson's son, who had been arrested for careless

driving. At that time, the son's uncles—the killer's brothers—were also questioned when a search of the DNA database revealed that they had the same Y chromosome. Following this trail of evidence eventually led to Hutchinson's arrest and conviction.

So far, I applaud every application of this database. But something makes me uneasy: what if Nazi Germany's Gestapo had had such a capability?

In the UK, local education authorities have a responsibility for tracking the progress of school children from different ethnic groups, with the laudable aim of addressing disadvantages in the school system. On a few occasions, representatives of fascist parties have been elected to city governments. If one day a fascist mayor asks, "Where are the Jews in this city?" it won't be possible for officials to answer, "We don't know," because these records include the name, race, and religion of every school-aged child.

Potential consequences

The IEEE Code of Ethics calls on members to "... 1. accept responsibility in making decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public

or the environment; ... 5. improve the understanding of technology, its appropriate application, and potential consequences; ..."

How far should we go in this? Which consequences are foreseeable, and which are too remote to be in the scope of our duty?

In particular, if we live in a more or less democratic country, are we entitled to assume that the sort of government we currently enjoy is likely to remain in place? I am in my fifties. My parents' generation was keenly aware that peace does not last, nor constitutions, nor rights. Public debate in the UK used to be influenced by many people who had fled Europe in the 1930s. Today's British technologists and policy makers have grown up in a period when war and dictatorship seem to be far away.

Dictatorship

So let's look at how dictatorship can work in a modern economy.

According to a 1943 report by the US Board of Economic Warfare, the German state bought 1.5 billion punched cards each year. IBM, which in effect had a monopoly on processing, printing, and producing punch cards, had built punch card printing presses and manufacturing

Continued on page 94

facilities in Germany during the 1930s.

The widening of the punch card to 80 columns was first proposed because of the large number of questions asked in a census ordered by the new Nazi government in 1933, a census outsourced to IBM. The technique of collation, an early equivalent to a join in a relational database, was developed because of the demand from both the new US Social Security Administration and the Nazi census offices.

The number tattooed on a concentration camp prisoner's arm was the key to a punched card recording the reason for incarceration, work skills, and other details. Card sorters played a key role in the

David Anderson observed that "computerized money is a dangerous thing if it is all ordinary citizens can use" (*Computer*, Sept. 2010, p. 7). In his reply, Olsen stated, "The German secret police managed to keep the population in the occupied territories, and in Germany, under strict control ... with no computers."

The SS, Gestapo, and other Nazi organizations made wide use of the best technology available to them. Without doubt, better technology would have made their control more complete and resistance more difficult.

The preceding sentence in Olsen's response to Anderson was, "There is, of course, always the

Today, if we choose to work on technologies that can be applied to social control, we can foresee the potential not only for benefit but also for terrible harm. If we make the assumption that dictators already have all the technical tools they could want, then we duck the responsibility to think these issues through.

RIPOSTE

As Chris Morris describes, a totalitarian dictatorship will use all available means to maintain control. For the Nazis, this meant having vast archives of data collected before and during the war. They introduced passports, permissions, war currency, and rigorous control of all travel. Newspapers and radio were under severe censorship. All available technology, everything from typewriters to telex, was used to make the administration effective. Yes, they also used punched card systems, a technology that had its origin in the 18th century, and was used for the US census as early as 1890. But punched cards are not computers.

Today, a suppressive regime will, of course, also use all available technology, perhaps including DNA, video surveillance, and control of movements. It might use computers to monitor communication and, for that matter, to follow monetary transactions.

Although no country currently has a full DNA archive of its citizens, governments could, at some point in the future, pass laws stating that everybody must offer a DNA sample "to protect society." But Germany's Nazi regime did not need either computers or DNA to persecute ethnic groups or political opponents; neither did Joseph Stalin to murder Polish officers and professors or Pol Pot to kill his own citizens in Cambodia.

If anonymous cash is important for a resistance movement, the regime can supervise transactions, perhaps also making the transition to a full

Laws for protecting privacy will only work as long as we have democratic governments that recognize the importance of the concept along with a free press as an additional safeguard.

"Extermination through Work" programs. These machines required a monthly maintenance visit by a technician from Dehomag, the German subsidiary of IBM (E. Black, *IBM and the Holocaust*, Dialog Press, 2008).

Nevertheless, Nazi domination of Europe was not complete. There was resistance, and it did make a difference. For example, an anti-Nazi newspaper was published daily in occupied Belgium.

In such a struggle, technologies aren't neutral. Since the 1940s, changes in printing technology and the development of the Internet have made it easier for citizens to publish, and harder for authorities to control what is published. On the other hand, the development of electronic databases has given authorities more oversight, and weakened the individual

Digital money

In response to Kai Olsen's comments about digital money,

risk that a democracy may go bad, but then rules and regulations, or practical measures, such as cash, will be of no avail." The spending of money was in fact one control point the Nazis did use. The Nazi state forbade people classified as Jews from working and took steps to ensure that those who didn't work starved. A complementary effort pressed shops not to serve Jews. If no financial transactions were anonymous, such policies could be implemented faster and more thoroughly.

We each have a choice about what projects we work on. Sometimes the most technically challenging projects are not the ones that will do the most good for humanity. For example, in the 1920s, a generation of brilliant people decided to devote their efforts to quantum theory, the greatest intellectual challenge of their day. They could not have known that within 20 years, this would lead to atomic weapons.

digital economy. The technology is available. Thus, laws for protecting privacy will only work as long as we have democratic governments that recognize the importance of the concept along with a free press as an additional safeguard.

Secrecy and the Internet

But there is another side to this. Today, the Internet and cell phones are important channels for getting information both out of and into a country. Twitter and Facebook played an essential role when the Egyptians ousted President Mubarak. The videos that show police and military brutality in Libya, Iran, and in other scenes around the world are important for the democracy movements.

In the case of Germany's Nazi regime, most of its atrocities were performed in secret, and there's strong evidence that concealment was a necessity. Today, this would not be possible. Thus, even the most brutal regimes must consider the risk of losing support by angering their citizens. Excessive brutality may also turn the outside world against the regime, inviting sanctions or, in some cases, an invasion.

Thus, technology can be the means either to suppress or to liberate. Personally, I'm an optimist. I see computer technology—whether it's the Internet, Facebook, Twitter, or smartphones—as offering important tools for advocating democracy.

Privacy and the Internet

But technology can be a threat to privacy even within the realm of a democracy. Video surveillance is an example. Cameras are used to secure banks or shops or to make it safer for us to walk the streets or ride on a bus. However, there are drawbacks.

A camera in an apartment building's parking area might reduce car theft or make it easier to find who bumped your car. At the same time, we don't want these videos to be used to see who came home

drunk. However, it's possible to have one without the other. Requiring that all data from cameras be stored on locked servers, and that only the police or an accredited security company can access those servers, would avoid many of the privacy problems.

Cash allows for anonymous monetary transactions. This anonymity is important for criminals, black market operations, and corruption. Clearly, it would be more difficult to buy drugs, sell stolen goods, or evade taxes if all transactions were digital and could be traced.

Cash also acts as bait for criminals. Many of the crimes perpetrated today, from muggings to robberies of gas stations, taxis, buses, shops, or banks are focused on cash. Removing cash doesn't eliminate crime, but it would eliminate many of the physical and psychological abuses of innocent people walking in the street or performing their jobs.


In Norway and Sweden, efforts are under way to accelerate the move toward a cash-free society. Interestingly, the unions for bank employees initiated and continue to drive this work. They feel a responsibility for removing the threat to their members that is associated with handling cash.

There may, however, be legal transactions that we want to keep private. There also might be expenditures that we want to hide from parents or a spouse, such as purchasing alcohol, pornography, or an expensive fishing rod. A society might also allow some leeway, even with transactions that are illegal, such as buying cannabis or sexual services. Without cash for these activities, politicians might have to take a stand where they previously had the chance to avoid the problem just by looking the other way.

Some might see this as an advantage, while others see it as a chance to reduce these types of activities. We need to seriously discuss what to allow or what to ban in a society.

If we decide that there are reasons to allow anonymous transactions as long as they're small—that is, based on the idea that small transactions have less impact on society than large ones—this can be achieved by retaining coins and small denomination bills when we move to a digital economy. The drawback is that we'll still have the expense of moving cash around, and many small sums might add up to be a problem in terms of both tax evasion and crime.

But we have a technical solution here as well. Using personal cash cards can provide anonymity for the buyer but not for the seller—the cash would go into the seller's bank account. That is, a digital economy doesn't necessarily imply an economy where every transaction is scrutinized.

Technology can't solve all privacy problems, but as we see, some solutions can make it easier to balance between the needs of society and individuals, perhaps resulting in a win-win solution. Of course, it all ends up with a question of trust. Do we trust the authorities to ensure our right to privacy? 

Chris Morris lives in Chester, UK. Contact him at chrismorris@acm.org.

Kai A. Olsen is a professor at Molde College and the University of Bergen and is an adjunct professor at the University of Pittsburgh. Contact him at kai.olsen@himolde.no.

Editor: Neville Holmes, School of Computing and Information Systems, University of Tasmania; neville.holmes@utas.edu.au

 **Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.**