Security, surveillance and counter-law

Richard Ericson reviews the changing face of the law relating to security and surveillance.

We live in insecure times, with problems with national security (threats of terrorism), domestic security (anti-social behavior), social security (benefit system fraud), and corporate security (liabilities for harm) at the top of the political agenda. Enormous expenditures on risk assessment and management ironically reveal the limits of risk-based reasoning and intensify insecurity. Images of catastrophe are fuelled, precautionary behaviour is pervasive, and extreme security measures are institutionalised in the form of 'counter-law.'

The notion of counter-law includes both 'law against law' and surveillance. New laws are enacted, and new uses of existing law are invented, to erode or eliminate traditional principles, standards and procedures of criminal justice. New surveillance infrastructures are developed, and new uses of existing surveillance networks are extended, to also erode or eliminate traditional principles, standards, and procedures of criminal justice. The two forms of counter-law treat everyone as if they are guilty of criminal intent. They criminalise not only those who actually cause harm, but also those merely suspected of being harmful, as well as authorities deemed responsible for security failures.

An obvious example of counter-law is anti-terrorism measures. For example, the USA Patriot Act places no limit on presidential authority to criminalise 'unlawful enemy combatants,' including US citizens. Criminalisation can occur on the basis of categorical suspicion: the wrong face in the wrong place at the wrong time. There is also suspicion by association: someone is suspected because they know someone suspected. Those arrested can be detained without specific charges for an indefinite period, and subject to state-sanctioned torture. *Actus reus*, the principle that criminalisation must be based on a specified criminal act, is eliminated. There is not even a pretense of what might be termed *probabilis reus*: criminalisation based on actuarial knowledge of risk. There is only the counter-law principle of *finus reus*: when criminalisation appears necessary for security, no other justification is called for and legal principles are preempted, finished.

The USA Patriot Act also enables unprecedented powers of surveillance. Based on the premise that malicious demons may be sleeping anywhere, law enforcers are given far-reaching access to private spaces and communication networks. The old model of resourceful police intelligence is replaced with one of universal suspicion that spells the end of innocence. The strategy is to cast the net as widely as possible, identify suitable enemies, not worry about false positive identifications, drop any pretense of due process of law, and accomplish summary justice.

Counter-law was normalised in other fields of security well before 9/11. A prime example in the field of domestic security is measures to combat anti-social behavior in England and Wales. The legal definition of anti-social behavior is left purposefully vague, providing scope for whatever may be defined locally by neighbours or other undesirables as terrorism. The only statutory definition is in section one of the Crime and Disorder Act 1998: conduct 'causing or likely to cause harassment, alarm or distress'. The culprit is subject to an anti-social behavior order (ASBO) made in civil proceedings. This order not only obligates him or her to desist from the harmful activity, but also requires submission to surveillance-based regimes that restrict time, place, and association (curfew and ban orders), involve disciplinary programs of behavioral change (counseling and courses), and compel compensation (community service and restitution). Breach of the civil order can result in strict liability criminal proceedings and imprisonment. Sentencing for breach can take into account previous behavior that may be known through surveillance and hearsay but not proven in court, undermining fairness standards that punishment should be proportionate to proven offences and not be retrospective.

ASBO legislation was passed in the same year as the first human rights legislation in England and Wales. Some ASBO provisions were explicitly constructed to limit the scope and application of the rights stipulated in the Human Rights Act and its cousin, the European Convention on Human Rights. Again, counter-law appears as a response to the law itself, as a source of uncertainty. When law sustains high standards of due process, evidence, proof, and culpability, it creates a great deal of uncertainty in the capacity of the criminal justice system to prevent, discover, build a case against, and successfully prosecute criminal behavior. In the demand for greater certainty, the standards of criminal law are undercut, the lower standards of civil and regulatory law ascend, and the urge to broaden and deepen surveillance intensifies.

Counter-law is also evident in the field of social security. In my home province of Ontario, Canada, the Ontario Works Act of 1997 shifted social benefits from a welfare needs-based system to one of temporary assistance to the unemployed person actively committed to seeking work. This legislation requires the claimant to enter into a 'participation agreement' similar to the contract-

based governance of ASBOs. They must consent to surveillance of personal circumstances, grant access to personal records in various institutions, and accept random home checks and substance abuse screening. The agreement also includes employment-related activities such as job searches, skills training, and acceptance and maintenance of employment. The implementation of this regime was accompanied by deep cuts to benefits. Taking inflation into account, there was a 34 per cent decline in the purchasing power of benefits between 1995 and 2002. In 2003, a single person received benefits at 65 per cent below the poverty line, a single person with a child was at 44 per cent below.

At the same time there was a shift from seeing welfare fraud as a minor but inevitable aspect of the benefits system, to treating all welfare as a kind of fraud against the commonwealth and therefore in need of stringent control. The crackdown included additional legislation in 2000 that made a claimant convicted of benefits fraud permanently ineligible for future benefits, giving in effect a life sentence of poverty without parole. The surveillance 'package' was elaborated to scrutinise the minutiae of the claimant's life. Unreported cohabitation, gifts, casual work paid in cash, or too many visits to the food bank might constitute fraud. Eligibility review officers operate with full search powers, including warrants, and an obstruction of investigation provision whereby anyone – the claimant's family, friends, neighbours, landlord, employer, or teachers – giving false information or otherwise interfering with an investigation - is subject to criminal sanction. Data matching systems across institutions red flag suspects for further investigation. A 'snitch line' was established which, in the 2001/02 reporting year, led to 6,527 investigations of claimants.

Government data for 2001/02 indicate that two-thirds of 35,452 fraud investigations were unfounded, and that where there was a problem the typical solution was summary administrative justice through reduction or termination of benefits. This data suggests that in most cases, 'governing through fraud' functions primarily as a means of obtaining acquiescence to surveillance and claims suppression. At the same time it is not surprising that some 'fraud' – in the form of unreported cohabitation, gifts, and informal economy income – is easy to uncover when claimants are kept so far south of the poverty line that they cannot survive without such activities.

No one escapes counter-law, including corporate 'actors' far north of the poverty line. Corporate activities with potential for catastrophic loss are at the forefront of the politics of security, surveillance, and counter-law. Controversies rage over the security of food supplies, medical services, nuclear, biological and chemical production, financial institutions, and environments. The response is counter-laws that criminalise corporate officials deemed responsible for catastrophe, even if they had no control over, or knowledge about, practices that led to the catastrophe, and even if these practices were widely regarded in corporate culture as acceptable before the catastrophe. A rotten apple view of rogue employees is extended to the corporate entity as a rotting barrel. Corporations are depicted as aggrandising monsters seeking only profits and leaving destruction in their wake. This anthropomorphisation of the corporation as pathological constructs a view of it as criminal. This view is radically different from the one that has traditionally granted the corporation enormous rights and privileges. Various forms of group liability, for example regarding conspiracy and incitement, are constructed. There are also efforts to make corporate manslaughter a statutory offence, as has occurred in the UK with the Corporate Manslaughter and Corporate Homicide Bill.

These manifestations of counter-law are nascent and largely symbolic, feeding into the rituals of visible precaution that characterise the politics of security, surveillance and counter-law. The real counter-law revolution is taking place at the level of surveillance-based internal controls of corporate conduct. These controls are enabled through legislation such as the Sarbanes-Oxley Act that followed Enron and other corporate scandals in the USA. New surveillance technologies, inspections, audits, and private policing expand after each catastrophic loss. Organizing organisations – state regulatory bodies, professional associations, industry associations, insurance bodies, and internal control units – proliferate as part of the frenzy to risk manage everything through corporate surveillance and criminalise those deemed responsible for security failures. Through these new mechanisms of surveillance, the corporate world has become more visible and subject to regulation than ever before. However, the resulting emphasis on risk aversion, defensive compliance, and reputation management fosters a corporate culture of deep suspicion. Employees feel criminalised because their everyday environment of security, surveillance and counter-law treats them as if they are operating with criminal intent.

Ironically, when law and other democratic institutions are most threatened by seemingly intractable problems, the response is to devise new forms of counter-law that further threaten those institutions. Law is transformed into an institution of suspicion, discriminatory practices, invasion of privacy, denial of rights, and exclusion. To borrow the legal definition of anti-social behavior, law itself becomes a source of 'harassment, alarm and distress.' Security trumps justice, and insecurity proves itself.

■

Richard Ericson *is Professor and Director, Centre of Criminology, University of Toronto.*

References

Ericson, R.V. (2007) *Crime in an Insecure World.* Cambridge: Polity.

Haggerty, K.D. and Ericson, R.V. eds. (2006) *The New Politics of Surveillance and Visibility.* Toronto: University of Toronto Press.