Editorial

Marking the end of a long association between the *Journal of Law, Information and Science* and the Faculty of Law at University of Tasmania, this general issue brings together a diverse range of articles. From human enhancement technologies to self-driving cars, and from big-picture philosophically-oriented questions to questions about detailed technicalities of black letter law, this general issue truly highlights how vast a field that law, science, information, and technology spans.

In the first article, Bebhinn Donnelly-Lazarov probes what it actually means to be responsible for 'action' in law because, without an answer, criminal law may incorrectly hold defendants 'responsible' for offences. She argues that 'action' should be conceptualised as made up of all the mental and physical elements of an offence. This composite definition, she argues, is more legally viable and philosophically coherent than dominant alternatives, such as paradigms that see physical movement as the foundation of human behaviour and that split physical movement from states of mind. In Donnelly-Lazarov's definition, crimes *are* actions, and it is for these actions that defendants are responsible.

Moving from Donnelly-Lazarov's broad-reaching topic, the next four articles relate to a narrower field of discussion: bio- or human enhancement technologies. Both Donnelly-Lazarov's article and this subset of articles — with the exception of Elves' piece on public confidence in policy-making — have been available online on the *Journal's* website for some time as part of a special edition on neurolaw.

First, Ana Nordberg seeks to turn 'human enhancement' into a legal concept that is clearly defined and normatively neutral. This legal concept can then serve as a tool to clarify what is already regulated by existing fields of law, and in turn to determine whether a new field of 'enhancement law' is justified. Down the line, the tool can help frame and develop substantive legal norms in this new regulatory field. Nordberg ultimately creates the concept of 'induced human evolution' — the use of technological means by humans to induce a specific result that improves, modifies, or introduces in the human body aesthetic features; physical, emotional or cognitive performance levels; and abilities. The change can be positive, negative, or neutral, but must be subjectively *intended* and done in an attempt to achieve some *permanent* evolutionary result.

Also with a view to assisting the regulation of human enhancement technologies, Hannah Maslen looks at how different disciplines can best inform policymakers and regulatory agencies. Focusing on lawyers, philosophers, and scientists, Maslen emphasises the need for inter-disciplinary collaboration but recognises

how their research approaches differ — scientists focus on factual descriptions, lawyers on what the law says, and philosophers on normative value claims. To reconcile these differences in a way that best facilitates the making of concrete policy recommendations, Maslen suggests that collaborative research questions must be more narrowly-defined. Specifically, they must focus on a particular technology in a particular context (eg, surgeons using cognitive enhancers that remedy fatigue-related impairments), and be informed by technological and legal realities (eg, the limits of a regulatory agency's authority).

Continuing the topic of policy-making, Charlotte Elves explores the importance and treatment of public confidence in the regulation of life sciences. She uses the regulation of human/animal hybrid embryos and of *in vitro* embryonic research in the UK as illustrations, and argues that political and legislative processes have diminished public confidence. From flipping legislative positions to the way that policy is debated in parliament, the public are led to believe that policymakers determine the permissibility of a novel technology based on technological capabilities of the time (what science *can* do), rather than on an assessment of societal and ethical implications (what science *should* do). Elves then proposes methods to avoid this misleading impression so as to promulgate effective, future-proof, and ethically sound policy for enhancing technologies.

In the final article on neurolaw, Elizabeth Shaw turns to the *use* of enhancement technologies. She explores the question of whether giving offenders biomedical moral enhancements (such as drugs that lower aggression) diminishes the moral worth of their future law-abiding behaviour — if an intervention makes one incapable of doing evil, does doing good still carry moral worth? Shaw draws on the communication theory of punishment, which implies that law-abiding behaviour after offending will only have moral worth if it emerges from an effortful process of repentance. She concludes that it would only be acceptable to use enhancements *on top of*, but not *in replacement of*, communicative punishment, and argues that this conclusion has practical implications in reducing political and economic motivations for using biomedical interventions in criminal justice.

Turning to self-driving cars, Maurice Schellekens considers the privacy law implications of vehicular safety warning systems — technology that allows vehicles to automatically detect and respond to dangers by communicating with nearby other vehicles and infrastructure. While vital for safe self-driving cars, these systems necessarily involve the frequent sharing and processing of data, including the car's location. Using the European Union's data protection framework, Schellekens analyses whether there exists a lawful ground for this data processing. While he shows that many grounds are impracticable here, he finds it a feasible option to create a legal duty to participate in location sharing and suggests to legislators that it is 'not unwise to get in lane' for this future.

Many articles in this issue discuss relatively novel technologies. However, Adam Day evaluates something more familiar: search engines. After a user inputs a query, search engines generate results through an automated process by an

algorithm. By analysing the recent High Court case of *Trkulja v Google* along with existing case law and commentary, Day considers whether search engine operators can, or should, be held liable for when those search results are defamatory. He agrees with the High Court that search engine results *can* convey defamatory imputations when viewed by the ordinary reasonable user, but makes contributions about what knowledge this reasonable user can be said to hold. However, as to whether the operators are liable as publishers and protected by defences (such as innocent dissemination, like newsagents), Day generally agrees with the Court of Appeal's affirmative findings. However, he diverges on who must plead the defence. Here, Day agrees with the High Court — the defendant operator, not the allegedly-defamed plaintiff, must argue it.

The final article in the issue is a co-authored piece by James Scheibner, Marcello Ienca, and Effy Vayena on data security of electronic health records ('EHRs'). They explore how distributed ledger technology ('DLT') can help satisfy data protection 'auditability' requirements for EHRs — requirements that it be possible to track which users have accessed a particular health record, when this was done, whether they had permission to do so, and so on. After a comparative study of five jurisdictions, the authors find a lack of uniformity about precisely what 'auditability' requires, as well as other complicating factors when using DLT. Therefore, they conclude that the technology can only be used to *supplement* rather than *oust* existing data protection legal frameworks and technical standards governing auditability. Nevertheless, as they demonstrate using three case studies of patients, physicians, and researchers accessing and using EHR data, the authors find that DLT *can* aid in improving how EHRs are managed.