GUIDANCE

Commerce Commission Guidance: **Algorithmic Collusion and the Commerce Act**

November 2026

COMMERCE COMMISSION NEW ZEALAND
Te Komihana Tauhokohoko

Purpose

This Guidance explains how the Commerce Commission approaches algorithmic collusion under the Commerce Act 1986.

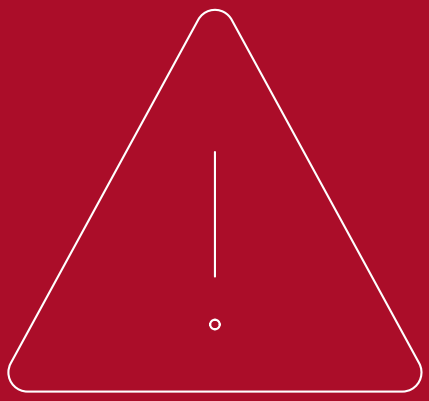
It is intended to help businesses understand how the use of algorithms, and technologies that rely on algorithms such as artificial intelligence (AI) systems and automated pricing systems, can potentially lead to cartel conduct in breach of the Commerce Act. It also outlines some suggested competition law guardrails for businesses using algorithmic tools and AI, to help them comply with the Commerce Act.

This Guidance is not law and is not intended to be legally binding or to replace legal advice. It does not provide an exhaustive statement of the law or of all circumstances in which algorithmic collusion may arise. Whether conduct breaches the Commerce Act will depend on the particular facts of each case.

Businesses remain responsible for ensuring that their use of technologies complies with competition law. The use of algorithms or AI does not change a business's obligations under the Commerce Act or shield it from liability where technology is used to facilitate cartel conduct.

Businesses can contact the Commission at **contact@comcom.govt.nz** to discuss potential competition law issues. We also encourage businesses to seek independent legal advice where appropriate.

If your algorithm breaks the law, so do you.



Introduction

Businesses are increasingly using algorithms, and technologies that rely on algorithms such as AI, machine learning systems and automated pricing tools, to make or support commercial decisions.

These technologies can deliver significant benefits by improving efficiency, enabling faster responses to market conditions, and reducing business costs.

However, algorithms can also create new avenues for collusion between competitors. Algorithmic collusion occurs where algorithms are used to facilitate, implement, monitor, or sustain coordination between competitors in a way that reduces competition. This may include situations where competitors agree to use the same algorithm, use different algorithms in a way that leads to coordination, exchange commercially sensitive information through digital systems, or use algorithms to monitor and enforce a collusive arrangement.

The cartel prohibition of the Commerce Act applies regardless of whether commercial decisions are made by people, algorithms, software, or AI systems. Businesses cannot avoid liability by delegating pricing or other competitive decisions to technology. Where an algorithm is used to facilitate cartel conduct, the businesses deploying or directing that technology may be held responsible.

As algorithms become more sophisticated and widely adopted, businesses should consider whether their design, implementation, and use could increase the risk of coordination with competitors. Appropriate governance, oversight, and competition law compliance measures can help businesses realise the benefits of these technologies while reducing the risk of algorithmic collusion.

This Guidance outlines the Commission's views on algorithmic collusion and provides guardrails to help businesses identify and manage competition law risks arising from the use of algorithms and AI systems.

Whether commercial decisions happen in the boardroom or the server room, businesses must ensure competition law compliance every step of the way.

What is algorithmic collusion?

Algorithmic collusion occurs when algorithms (including technologies that rely on algorithms) facilitate, support, or sustain anti-competitive coordination between competitors.



Algorithmic collusion and cartel conduct under section 30 Commerce Act

Section 30 of the Commence Act prohibits entering into, or giving effect to, a contract, arrangement, understanding, or covenant containing a cartel provision. A cartel provision is one with the purpose, effect, or likely effect of fixing prices, restricting output, or allocating markets between competitors.

Cartel conduct may result in significant civil penalties and can give rise to criminal liability, with potential penalties including imprisonment for individuals and substantial financial penalties for businesses.



Implementation of a cartel using algorithms

The clearest application of section 30 arises where competitors explicitly agree though humans to coordinate prices, customers, territories, output, or bidding behaviour and then use algorithms to implement, monitor, or enforce that agreement.

For example, competing businesses owners might agree that prices will be maintained above a certain level and then use automated pricing software to ensure compliance in real time. In these circumstances, the algorithm is simply a tool used to implement cartel conduct. The fact that pricing decisions are automated would not prevent the arrangement from contravening section 30.

Competitors who enter into cartel agreements, and use algorithms to implement the agreement, will be liable under section 30 of the Commerce Act in the usual way.

Case study

Amazon posters case: In 2015/16, UK and US authorities took action against an online seller for a price fixing agreement that was implemented by an algorithm. Competing online sellers of posters agreed not to undercut each other's prices on Amazon Marketplace, and used an algorithm to implement and monitor the agreement. The case demonstrates that businesses using algorithms and AI are not shielded from competition law liability where this technology is used to implement or support a cartel agreement made by humans.

The use of algorithms, AI systems, or automated pricing tools does not alter the application of section 30. The key question under section 30 remains whether there is a contract, arrangement, or understanding between competitors that results in a cartel provision.

We list below scenarios where algorithmic collusion may be captured by section 30.



Facilitation of a cartel through independent, shared algorithms and platforms (hub-and-spoke collusion)

Competition law risks may also arise where competitors rely on the same independent algorithm, pricing platform, data intermediary, or software provider.

If a shared algorithm or platform facilitates the exchange of commercially sensitive information between competitors, or generates pricing recommendations using competitors' confidential pricing information, this could support the existence of an arrangement or understanding between competitors.

Businesses should not assume that the use of an independent algorithm or platform insulates them from liability. A business may breach the Commerce Act even where coordination occurs, and an arrangement or understanding is facilitated, through an intermediary product.

Case study

RealPage case: In 2025, US authorities alleged that competing landlords had engaged in price fixing by using a common pricing software. That software relied on the landlords providing it with non-public, commercially sensitive information to generate rental pricing recommendations, enabling the landlords to align pricing. In response Realpage made significant changes to its software. This case highlights the importance of ensuring businesses make their own pricing decisions, and do not use common algorithms or AI systems in ways that facilitate the sharing or use of competitors' sensitive information.

The decision-maker may be an algorithm, but the law remains the same.

Technology may be moving fast, but it hasn't outrun competition law.

Facilitation of a cartel through sharing of sensitive information

The price-fixing prohibition in section 30 is broad.



It captures agreements relating not only to final prices,
but also discounts, rebates, allowances, credits, and other components of price.

Accordingly, concerns may arise where business' pricing algorithms are trained, calibrated, or operated using current or future competitively sensitive information obtained from competitors. Whether section 30 is engaged will depend on the specific facts, including the type of information obtained or shared, and how that information is used.

If competitors share information about current or future pricing strategies, and that information reduces competitive uncertainty and enables coordination, the arrangement risks being cartel conduct captured by section 30. This applies whether the shared information is used by humans making pricing decisions for the business, or by algorithms and AI systems making or implementing pricing decisions.



Autonomous pricing systems entering into cartel agreements

Emerging autonomous pricing systems, that are AI-driven and rely on algorithms, can make increasingly sophisticated pricing decisions with limited human oversight or influence. In some circumstances, separate systems that are deployed by competitors may self-learn to interact and produce coordinated market outcomes with each other, which resembles collusion. This may occur without the knowledge of the businesses, or without the business even being aware that the systems are capable of collusion. Research suggests that advanced autonomous pricing systems can, under certain conditions, converge towards supra-competitive pricing outcomes.

When assessing potential collusion between autonomous pricing systems, the Commission would assess whether there is evidence of a contract, arrangement, or understanding between competing businesses, including through means such as algorithms and information sharing arrangements, as outlined above.

The Commission notes that section 90 of the Commerce Act attributes liability to a business for the conduct of their agents where that person is acting within the scope of their actual or apparent authority.

Designers, manufacturers and retailers

Designers, manufacturers and retailers of algorithmic tools and AI can also be liable under section 30, for being a party to, or giving effect to, cartel conduct. They can also face accessory liability under section 80 if they aid, abet, counsel, procure, induce, or are knowingly concerned in cartel conduct.

Early reporting of competition concerns can help identify and address risks before significant harm occurs.

The Commerce Commission's approach

The Commerce Commission recognises that algorithmic tools and AI can deliver significant benefits for consumers and businesses. Our focus is not on the adoption of this technology in itself, but on use that has the potential to harm competition.

The Commission will continue to monitor developments in the use of algorithms and AI systems by businesses, and may investigate conduct where systems facilitate cartel conduct or other anti-competitive outcomes. Businesses should ensure they understand how their systems operate and take proactive steps to remain compliant with the Commerce Act.

Businesses concerned about potential cartel conduct should seek legal advice and consider engaging with the Commission at an early stage. Early reporting of competition concerns can help identify and address risks before significant harm occurs.

To assist businesses, we provide below suggested guardrails for using algorithms and AI.

Competition law guardrails for businesses using algorithmic tools and AI

As businesses consider the governance arrangements needed for the safe deployment and use of algorithmic tools and AI systems, they should also assess and manage any competition law risks that may arise. The guardrails set out below are not exhaustive, but are suggested approaches businesses could adopt as part of their broader governance, compliance, and oversight processes for using this technology.

Maintain independent commercial decision-making: Businesses should ensure that pricing, output, customer targeting and other competitive decisions remain independent from competitors. Algorithms and AI systems should not be designed, trained or configured to coordinate with competitors or respond to competitor conduct in a manner that facilitates collusion.

Prohibit the use of competitors' sensitive information: Algorithms and AI systems should not be trained on, calibrated using, or provided with competitors' sensitive current or future pricing, output, customer or strategic information, unless permitted by law. Businesses should have controls in place to identify and prevent the use (including inadvertent use) of competitively sensitive competitor information.

Establish human oversight: Appropriate human oversight should be maintained, particularly where pricing or output decisions are highly automated. Human oversight should involve meaningful review and challenge of system outputs, rather than simply rubber-stamping recommendations. Staff responsible for commercial decisions should understand how a system operates, regularly review the operation of the system to ensure no unexpected and contravening conduct is occurring, and be able to promptly challenge or override a decision and recommendations of the system where necessary.

Conduct due diligence on third party products: Before adopting third party algorithms, pricing software or AI-based decision tools, businesses should understand:

- what data is used by the system
- whether competitor information contributes to outputs
- how recommendations are generated
- whether data from different businesses is pooled or ring-fenced in the system
- the governance arrangements applied by the provider
- what safeguards exist to prevent anti-competitive outcomes
- whether there have been any past issues that may risk breaching competition law

Businesses should question and carefully assess whether the third party product could facilitate the sharing of commercially sensitive information or align pricing decisions across competitors.

Conduct regular competition compliance audits: Businesses should periodically review their:

- algorithm design and objectives
- data sources and inputs
- pricing recommendations and outcomes
- interactions with competitors
- third-party data sharing arrangements
- compliance controls

Audits should specifically assess whether systems could facilitate information exchange, coordinated conduct, or reduce competitive uncertainty with competitors. Autonomous self-learning systems in particular should be regularly reviewed, and where an algorithm or AI tool is authorised to increase prices for which goods or services are offered for sale.

Implement and maintain compliance programmes: Businesses should ensure their compliance programmes and training cover algorithmic and AI-related competition risks, and ensure employees understand competition law obligations when adopting and using algorithmic and AI technologies. Where staff identify potential anti-competitive outcomes, unexpected algorithmic behaviour, or concerns regarding information sharing with competitors, the issue should be escalated immediately.

Maintain documentation: If possible, businesses should consider keeping records demonstrating:

- how algorithms are designed and governed
- the sources of data used by the system
- competition law risk assessments
- audit findings and remediation actions
- decisions to adopt or modify algorithmic pricing tools

This is a guideline only and reflects the Commission's view. It is not intended to be definitive and should not be used in place of legal advice. You are responsible for staying up to date with legislative changes.

You can subscribe for information updates at **www.comcom.govt.nz/subscribe**

Contact us with information about possible breaches of the laws we enforce: Phone: **0800 943 600**
Write: **Enquiries Team, PO Box 2351, Wellington 6140** Email: **contact@comcom.govt.nz** **www.comcom.govt.nz**